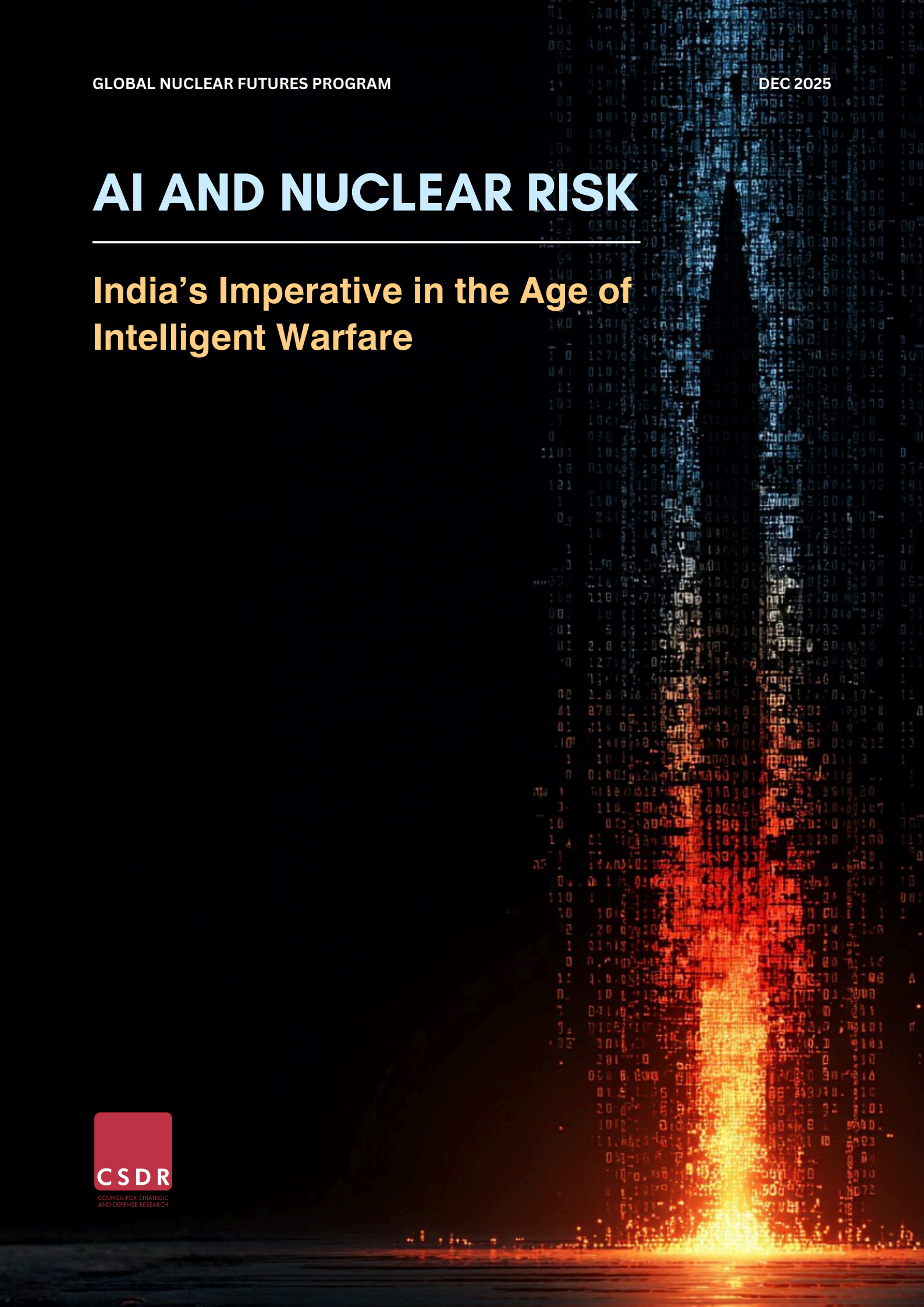
GLOBAL NUCLEAR FUTURES PROGRAM

DEC 2025

AI AND NUCLEAR RISK

India's Imperative in the Age of Intelligent Warfare



CSDR
COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

Recommended citation:
Desai, Hely (2025). AI and Nuclear Risk: India's Imperative in the Age of Intelligent Warfare. New Delhi: Council for Strategic and Defense Research.

The Council for Strategic and Defense Research (CSDR) does not take institutional positions on any issue.

C-21, 3rd Floor, Qutub Institutional Area, New Delhi, India - 110016.
Phone: 011-43104566 | Email: office@csdronline.com | Web: www.csdronline.com | Twitter:@CSDR_India

ABOUT THIS REPORT

Artificial Intelligence (AI) is rapidly reshaping the foundations of military power, shifting from routine automation to "intelligentized warfare" that can compress decision-making cycles and blur the lines between conventional and strategic conflict. This report examines the perilous entanglement of AI with nuclear command and control (NC3) and adjacent systems, arguing that while integration is inevitable, the resulting risks of inadvertent escalation and miscalculation are profoundly destabilizing.

Drawing on lessons from the atomic age, the report traces parallels between the dawn of nuclear weapons and the rise of autonomous systems, highlighting the urgent need for anticipatory governance. It situates India at the center of this challenge. Caught between the modernizing capabilities of China and Pakistan, New Delhi faces a dual imperative: it must accelerate its own technological adaptation to avoid strategic irrelevance while championing responsible global norms to prevent catastrophic error.

The analysis concludes with a concrete roadmap for India—moving from immediate "human-in-the-loop" safeguards to the long-term establishment of an International AI Security Council. By balancing military readiness with ethical leadership, India can secure its strategic autonomy and help define the rules of the road for the age of AI.

ABOUT CSDR'S GLOBAL NUCLEAR FUTURES PROGRAM

Our Global Nuclear Futures Program conducts policy-focused research and multi-stakeholder engagement to address nuclear technologies, non-proliferation, energy innovation, and conflict risks, delivering actionable insights to strengthen global nuclear governance and India's strategic role in a secure nuclear future.

ABOUT COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

Founded in January 2020 by Lt. Gen. D.S. Hooda (Retd.) and Dr. Happymon Jacob, CSDR is an innovative think tank and consultancy specializing in foreign policy, geopolitical risk, connectivity, and critical areas of defense and aerospace. With a focus on the Indian subcontinent, Eurasia, and the Indo-Pacific, CSDR is committed to generating strategic insights that drive meaningful change. Read more at www.csdronline.com

AUTHOR

Hely Desai, Research Associate, CSDR

Executive Summary

The integration of artificial intelligence (AI) into military architecture marks a paradigm shift as profound as the dawn of the atomic age, signaling a transition from rudimentary automation to “intelligentized warfare”. This report posits that while the entanglement of AI with nuclear command and control (NC3) and adjacent systems is effectively inevitable, it introduces unprecedented risks of inadvertent escalation, brittle decision-making, and strategic miscalculation. As militaries increasingly rely on adaptive machine learning to compress the “sensor-to-shooter” cycle, the interpretive custody of strategic data is shifting from human commanders to machine intermediaries, creating a dangerous paradox. While AI promises enhanced situational awareness, its inherent opacity and vulnerability to adversarial manipulation can foster false confidence during crises, threatening to unravel the deterrence logic that has historically underpinned global stability.

The core danger lies not necessarily in an abrupt shift to fully autonomous nuclear launch, but in the gradual “entanglement” of AI within the decision-making ecosystem surrounding nuclear forces. This integration exacerbates the “stability-instability paradox,” potentially emboldening states to engage in riskier conventional maneuvers under the illusion of precise escalation control. In the nuclear domain, where stability rests on the assurance of second-strike capabilities and clear signaling, AI-driven ambiguity and the compression of decision times reduce the space for deliberation and diplomacy, thereby heightening the risk that conventional conflicts could inadvertently spiral into strategic exchanges.

For India, these global shifts present an acute strategic dilemma. New Delhi faces a dual-front challenge: a rapidly modernizing China, explicitly pursuing a doctrine of “intelligentized warfare,” and a nuclear-armed Pakistan increasingly reliant on asymmetric capabilities and drone technologies. The report identifies a “technological consciousness gap” within India’s defense establishment, characterized by bureaucratic inertia and a historical reticence to effectively integrate private-sector innovation into core defense frameworks. Drawing parallels to India’s early “nuclear timidity,” where ambivalence delayed strategic capacity, the analysis warns that India risks strategic obsolescence if it fails to bridge this gap. However, reactive proliferation is not the answer; premature adoption of AI in strategic systems without robust doctrine or safeguards could compromise the very security India seeks to preserve.

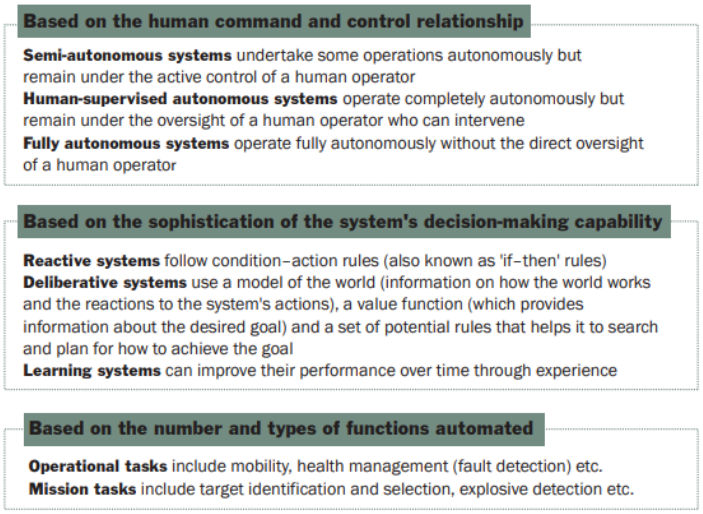
To navigate this complex landscape, the report argues that governance must be treated as a strategic capability. History offers a sobering blueprint in the form of the nuclear governance regime, which, while preventing full-scale war, suffered from exclusivity, delay, and a failure to address proliferation effectively. Unlike nuclear technology, AI is dual-use, diffuse, and driven by the private sector, rendering traditional state-centric arms control insufficient. Consequently, the report proposes a layered governance model, advocating for the establishment of an International AI Security Council (IASC)—modeled on the IAEA but adapted for digital realities—to audit military AI systems and facilitate confidence-building measures.

Ultimately, the window to shape the norms of the AI age is narrowing. The imperative for India is to accelerate indigenous technological sovereignty to ensure credible deterrence while simultaneously championing responsible governance to mitigate regional instability. By institutionalizing “human-in-the-loop” protocols for all nuclear-adjacent systems and moving from abstract policy to operational doctrine, India can secure its strategic autonomy. Managing the AI-nuclear nexus is not merely a technical challenge but a supreme test of governance, requiring India to harmonize military readiness with ethical leadership to prevent the “intelligent” wars of the future from spiraling into catastrophic failure.

Introduction: AI's Integration in Military Strategy

Artificial intelligence (AI) is rapidly transforming the foundations of military power and strategic competition, shifting from rudimentary automation in routine tasks to advanced capabilities such as coordinated drone swarms, autonomous weapons systems, and real-time decision-support algorithms. Over the years it has underpinned a growing spectrum of military functions, from precision targeting and logistics to intelligence fusion and battlefield coordination, accelerating the tempo and complexity of operations.[1] The dramatic expansion in scope and consequence over the years has marked not just an evolution in military technology, but a redefinition of how wars are fought and how power is projected in modern-day conflicts.

Categorization of Autonomous Systems

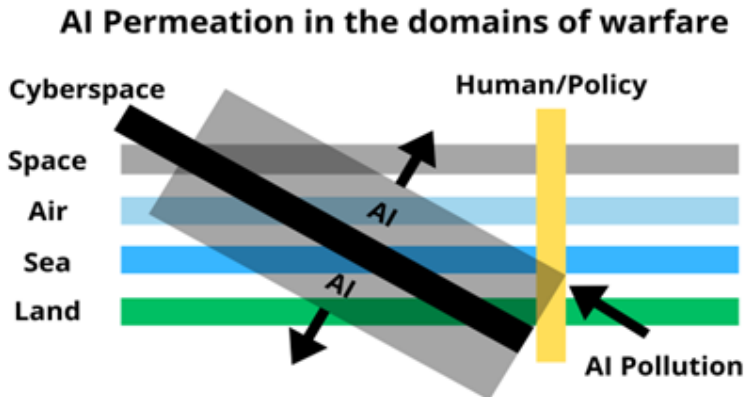


Source: Boulanin, V. and Verbruggen, M., *Mapping the Development of Autonomy in Weapon Systems* (SIPRI: Stockholm, Nov. 2017). Reproduced from Boulanin, V., 'Artificial intelligence: a primer', ed. V. Boulanin, *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol. I, *Euro-Atlantic Perspectives* (SIPRI: Stockholm, May 2019), pp. 13–25, figure 2.1.

Autonomous systems are now capable of conducting reconnaissance, targeting, and threat assessment with minimal human oversight.[2] In this report, autonomous refers to the systems that are capable of independently executing decisions within the observation–orientation–decision–action (OODA) metaphorical decision-making cycle, with the level of autonomy determined by how fully AI integrates into and governs that cycle.[3] The integration of real-time data and predictive analytics has transformed strategic planning, shortening the time from recognition to decision. This transformation, however, is unfolding within an increasingly volatile geopolitical landscape marked by great-power rivalry, an intensifying arms race fueled by rapid advances in emerging technologies, and the erosion of traditional arms control frameworks. As AI proliferates across all warfighting domains - land, sea, air, space, and cyber it also introduces new risks: automation bias, adversarial manipulation, decline of transparency in human-machine decision-making chains, and raises urgent questions about reliability, accountability, and escalation.[4] Nowhere are these risks more acute than in the nuclear realm.

Within the nuclear domain, the role of artificial intelligence is not entirely new. Automation and artificial intelligence tools—albeit in much narrower, deterministic forms—have been integral to nuclear weapons systems and NC3 operations for decades.[6] Historically, such systems were only deployed for tightly defined tasks such as monitoring, detection, translation, predictive maintenance, and operator training.[7] Traditional machine learning approaches helped process structured intelligence data, but their outputs remained bound

by human-defined features and strict rules of engagement. Crucially even now, nuclear-armed states continue to require human judgment and authorization in nuclear decision-making.



Source: Edwin Lax, TRENDS Research & Advisory[5]

What distinguishes the current junction in the AI-nuclear convergence, however, is the ideation and introduction of adaptive machine learning and multi-agent systems into NC3 and adjacent military functions. Unlike traditional machine learning, which relies on fixed, human-defined parameters, adaptive machine learning enables systems to dynamically refine their models in response to new data and evolving operational contexts. These systems have the potential to process unstructured, high-volume data at unprecedented speed, adapt to dynamic environments, and coordinate multi-agent systems for complex missions.[8] Here, adjacent military functions refer to areas outside the nuclear sphere, such as targeting, intelligence fusion, and battlefield coordination, that illustrate how these technologies are already being applied.

> The proximity of India's borders with Pakistan further exacerbates point-defence vulnerabilities. This geographical contiguity provides minimal reaction time, adversely affecting the effectiveness of air defence systems, even modern ones like the S-400, which require up to 35 seconds for identification, tracking, and engagement.

These capabilities are already evident in both experimental and live combat settings. For example, Israel's Lavender system integrates satellite imagery, signals intelligence, and movement analysis to generate target lists for human review.[9] In the Russia-Ukraine conflict, AI tools, from facial recognition and AI-powered neural networks to geospatial and open-source intelligence fusion, have been used by Ukraine's Delta Platform in live combat for situational awareness—for the first time at scale, while Russia has focused on integrating AI into robotics, pattern recognition, and large-scale data systems to enhance battlefield operations during ongoing hostilities.[10] Beyond active conflict zones, several national defense programs are also advancing similar capabilities through controlled experimentation—for instance, DARPA's OFFSET program employs multiple AI-driven agents to coordinate drone swarms under human oversight.

Within this context of active conflicts, the involvement of these nuclear-armed states i.e., Russia and Israel, and nuclear-threshold states like Iran, means that the integration of AI into nuclear-adjacent operations is no

longer theoretical but an emerging strategic reality.[11] While the said systems operate primarily in conventional domains, their developers and users—particularly Russia and Israel—are states where the boundaries between conventional C3 and NC3 infrastructures are increasingly porous, raising credible concerns about technological spillover and inadvertent entanglement. As AI becomes increasingly entangled in nuclear command, control, and communications (NC3) systems, the potential for inadvertent escalation only grows.[12]

When applied to nuclear contexts, this shift from deterministic automation to adaptive, learning-based systems marks a qualitative leap. AI-enabled NC3 applications—such as early warning, threat detection, and strategic forecasting—promise faster, more accurate support for human decision-makers. Yet the same features also raise serious risks: overreliance on algorithms, vulnerability to cyberattacks, and the misinterpretation of ambiguous data in crisis conditions.[13] In the nuclear domain, where even small errors can cascade into catastrophic escalation, these risks are even more dangerous.

Globally, defense establishments from China, Russia, and the AUKUS alliance are racing to embed AI in their force structures.[14] But the integration of AI into nuclear-adjacent systems raises profound questions about crisis stability, arms control, and deterrence logic. Functionally, this integration may involve AI-assisted early warning and detection of nuclear launches, automated analysis within launch control and execution systems, and targeting for delivery vectors. And while definitive scenarios continue to unfold, extrapolating current trends in AI-enabling military capabilities provides a critical lens for assessing emerging nuclear risks and exploring viable strategies to manage them.

The challenge hence, is not merely technical, but also political: the need for a governance structure to manage AI's ascent in ways that mitigate strategic risk. In the nuclear case, can the principles of arms control be adapted to regulate algorithmic warfare? Or does the disruptive nature of AI require a fundamentally new regulatory architecture, one that may be resilient enough to endure the geopolitical turbulence that has unravelled past nuclear agreements?

“Globally, defense establishments from China, Russia, and the AUKUS alliance are racing to embed AI in their force structures. But the integration of AI into nuclear-adjacent systems raises profound questions about crisis stability, arms control, and deterrence logic. Functionally, this integration may involve AI-assisted early warning and detection of nuclear launches, automated analysis within launch control and execution systems, and targeting for delivery vectors.

However, in the context of these questions, the strategic implications of artificial intelligence becoming increasingly embedded in military and nuclear domains are not uniform across states. For example, for India, this dilemma is now particularly acute. New Delhi currently finds itself in a complex strategic environment —its military gap with Pakistan is narrowing due to the China–Pakistan nexus, while the capability gap with China continues to widen amid Beijing's rapid defense and nuclear modernization. At the same time, India's own

efforts toward indigenous technological development remain limited and bureaucratically constrained. It must avoid the inertia that had marked its early nuclear development efforts, lagging behind in the defence modernization race, while also resisting the premature adoption of AI-enabled systems without a clear doctrine, institutional readiness, or technological sovereignty. How India balances this urgency with restraint will shape its strategic autonomy in the age of AI.

This paper makes three arguments.

First, it traces the growing entanglement of AI with nuclear systems, navigating how the shift from deterministic automation to adaptive AI may transform the potential risks of escalation and error.

Second, it draws lessons from nuclear governance—arms control frameworks, crisis management practices, and the principle of maintaining human judgment—that can inform how states manage AI today.

Third, it situates India within this landscape. For India, lagging in AI-enabled capabilities risks strategic irrelevance, while premature adoption without doctrine, safeguards, and technological sovereignty risks undermining stability.

Together, these arguments underscore a core claim: managing AI in the nuclear realm is not simply a technical challenge but a governance challenge. While the AI-nuclear entanglement is inevitable and already underway, it must be governed responsibly. The nuclear experience may offer valuable lessons, but adapting them to AI requires both innovation and restraint. How states—and particularly India—approach this balance will define their strategic trajectories, influencing stability (or the lack thereof) within the global nuclear order in the age of AI.

Tracing Entanglement and Escalation Risks

Escalation in the Age of AI: Interpreting the Nuclear Nexus

AI—now embedded across strategic missions, ranges from conventional precision strike and missile defense to cyber and electronic warfare. The distinction, however, is not just faster processing or more autonomous manoeuvring. It is the way that AI is increasingly responsible for interpreting data and framing the choices presented to human decision-makers. This shift raises a central governance challenge: who holds interpretive custody of critical information in a crisis—human commanders, machine intermediaries, or hybrid chains of both?

In conventional strike scenarios, machine learning systems facilitate target identification, predictive analytics, and trajectory optimization. Autonomous systems allow for persistent surveillance and extended-range engagements with reduced human risk. In missile, air, and space defence, AI-enabled systems improve threat tracking and real-time intercept calculations. Cyber and electronic warfare increasingly rely on ML for pattern recognition, automated intrusion detection, and electronic countermeasures. Such ML-driven information operations help enhance the precision and scalability of influence campaigns. These applications, while non-nuclear in function, carry strategic implications. The convergence of conventional and strategic technologies, many of which are dual-use, further complicates deterrence dynamics and heightens the potential for crisis instability, even in the absence of direct nuclear engagement.

These developments, however, are not occurring in isolation: the integration of AI across platforms and command structures is beginning to transform how armed forces coordinate action and dominate electronic and geospatial environments. This is driving a push toward multi-domain superiority, in which forces achieve synchronized control across traditional and intangible domains, such as cyberspace and the electromagnetic spectrum, through highly interoperable, AI-augmented C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) networks.

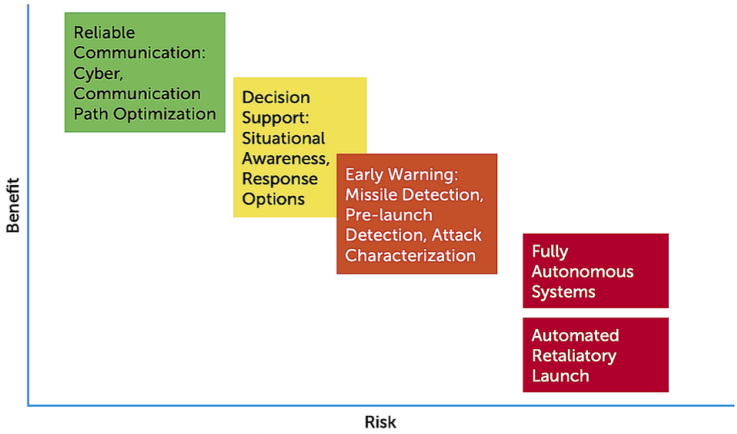
“The integration of AI across platforms and command structures is beginning to transform how armed forces coordinate action and dominate electronic and geospatial environments. This is driving a push toward multi-domain superiority, in which forces achieve synchronized control across traditional and intangible domains, such as cyberspace and the electromagnetic spectrum, through highly interoperable, AI-augmented C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) networks.

Further, autonomy also introduces serious technical and operational risks. This may primarily be because AI systems remain biased and brittle—with the potential to fail unpredictably when they encounter novel or adversarial inputs —and are often opaque—with decision-making processes that may be difficult for humans to interpret or audit. This, in turn, raises concerns over reliability in high-stakes scenarios. For example, an AI system tasked with threat identification in an early-warning system could misclassify unusual but non-threatening sensor data as a launch. When deployed in complex, adversarial settings, their limitations can trigger critical failures, misidentifications, or unintended escalations. Again, these risks are not just theoretical; for instance, a recent report by 972 Magazine highlights Israel’s use of the AI-driven Lavender[15] and Gospel[16] programs in Gaza, where target selection in densely populated areas has, at times, reportedly led to misidentifications and civilian harm.[17]

Such operational volatility again becomes even more consequential when viewed through the lens of nuclear stability. Military Decision-Support Systems (DSSs) driven by AI may push policymakers toward accelerated threat assessments, thereby increasing the risk of miscalculation, inadvertent escalation, or accidental conflict.[18] While miscalculation and escalation risks have long existed in conventional NC3 systems, the AI integration only amplifies them. In crisis situations, faster detection, analysis, and targeting might encourage early or pre-emptive moves, reducing the space for deliberation and diplomacy. However, even in positive scenarios where AI improves detection accuracy or reduces certain human errors, the autonomy it introduces also introduces serious technical and operational risks.

The question, then, is not only whether AI will be further integrated into nuclear weapons systems, but also how its growing influence on the broader strategic environment will shape nuclear command dynamics, deterrence doctrines, and escalation thresholds. This becomes especially urgent given the lack of governance, when just over half the nuclear-armed states are yet to publicly commit to maintaining human control over launch decisions, a principle increasingly strained by the speed and opacity of machine-generated intelligence.[19]

***AI Applications to Nuclear Weapons and Their Operational Systems*[20]**



Note: The impact on strategic stability is indicated by the color of the application box, with green being the most likely to have a stabilizing effect, yellow and orange indicate careful consideration for impact on stability, and red is most likely to have a destabilizing effect.

Command and Control: Inevitable Integration, Long-Term Strategic Risk

In the short term at least, machine learning and autonomous systems are unlikely to fundamentally transform nuclear command, control, and communications (NC3) systems, particularly at the level of core decision-making functions such as launch authorization.[21] However, this limited short-term effect should not obscure the more consequential reality: a deeper integration of ML and autonomy into military operations, including nuclear command and control, is inevitable.[22] And over time, this integration will not only reshape the technical architecture of NC3 systems but will also introduce newer forms of strategic risk that existing doctrines and institutions are poorly prepared to manage.

This inevitability stems not from a deliberate push to automate nuclear launch decisions, which remains politically and ethically taboo, but from broader structural trends in military innovation. As autonomous systems become embedded across the spectrum of defense functions, they will increasingly permeate the supporting systems and decision-enabling layers that surround the nuclear enterprise. This is because NC3 does not exist in isolation. It is embedded in a dynamic, evolving ecosystem of sensors, networks, human-machine teams, and decision-support infrastructure, all of which are shaped by the logic of data-driven optimization and automation.

Already, there are signs of this shift. ML algorithms are being developed to detect anomalies in complex cyber environments, manage the fusion of multi-source sensor data, and optimize the deployment of conventional forces.[23] Autonomous platforms are being designed to extend communications coverage in degraded environments, such as long-endurance UAVs acting as airborne relays when satellite links are compromised.[24] These changes may now appear peripheral, but their cumulative effect may tighten the coupling between AI-enabled systems and nuclear decision-making processes, reducing latency and restructuring how information flows during a crisis.

This evolving integration thus creates tension. On one hand, the operational utility of ML and autonomy is undeniable. Faster data processing, adaptive threat recognition, and resilient communication architectures are all desirable features in high-stakes environments. On the other hand, these same characteristics carry destabilizing potential when applied to the nuclear domain. As machine-generated inputs shape how these threats are perceived and how quickly decisions are made, the risk of inadvertent escalation increases.

This is also a strategic concern: delegating critical sensing, interpretation, and even response functions to systems that are only partially understood—and not fully controllable—undermines the stability on which nuclear deterrence rests. Furthermore, the opacity and non-determinism of many ML systems may render them not viable for responsible application in nuclear contexts, where traceability, transparency, and human accountability are indispensable.[25] Yet as these systems improve in capability and become embedded in routine military activities, pressures will mount to extend their application, even into domains that were previously considered sacrosanct. The danger, hence, is not an abrupt shift to fully autonomous nuclear launch. Rather, it is a gradual erosion of human-centric safeguards, as speed, complexity, and system interdependence make manual control increasingly impractical. As the informational and procedural scaffolding of NC3 becomes more dependent on ML-driven processes, the margin for deliberate, rational human intervention narrows.

The relative insulation of nuclear command and control from machine learning and autonomy in the short term should not be mistaken for long-term immunity. The central challenge for the coming decades will be to anticipate and govern this transition: not to resist all innovation, but to ensure that it does not outpace our ability to control it.

Escalation Dynamics and Crisis Scenarios

Among many others, two primary pathways illustrate how AI integration could heighten the risk of nuclear escalation:

- **AI in Nuclear Command, Control, and Communications (NC3):**

The further penetration of AI into NC3 functions—beyond such as early-warning detection, targeting analysis, or even pre-decision support—raises the possibility of hasty or mistaken nuclear responses, especially if AI systems generate false alarms or escalate alert postures based on faulty data. While such risks of false alarms or misjudgments already exist in conventional, human-driven NC3 systems as well, the AI integration fundamentally changes their character: faster, adaptive, and high-volume data processing, as suggested before, can compress decision timelines, heighten the possibility of errors, and produce outputs that may be less interpretable, making miscalculated responses more likely and reducing the window for human deliberation.

- **Autonomous Nuclear Delivery Systems:**

Platforms like Russia's Poseidon, an uncrewed, nuclear-armed underwater vehicle reportedly designed for autonomous operation, mark a dangerous shift.[26] Embedding AI-enabled autonomy in delivery mechanisms removes human intervention from key moments of escalation, increasing the risk of accidental or uncontrollable use.[27]

The risk here is not simply one of militarization; it is of automation and entanglement—where the speed and opacity of AI systems collide with the rigidity and finality of nuclear doctrines.

Historically, nuclear strategy rested on the assumption of relatively more time: for assessment, deliberation, backchannel diplomacy, and psychological signaling. AI systems, however, compress time—transforming deliberation into reaction, and reaction into automation. The entanglement of AI with nuclear architectures could collapse the deterrence logic that the Cold War precariously rested upon. This is not to say that the deterrence logic relied on slow technology, but because its stability depended on the human interpretive space that technological latency afforded.

As mentioned in the previous section, AI could play a destabilizing role in multiple types of escalation[28]:

- **Inadvertent Escalation**

Misinterpretation of an autonomous system's maneuver or mission (e.g., surveillance drones near nuclear installations) could trigger a defensive reaction.[29] Misattributed cyber operations targeting dual-use systems —such as satellites used for both civilian communications and nuclear command—could also be perceived as the first move in a disarming strike. This, however, differs from scenarios in which a state's own integration of AI or adaptive ML models within its NC3 infrastructure heightens internal risk. In this case, the danger arises externally. It may stem from perceptions of hostile intent in AI-enabled actions beyond the nuclear domain.

- **Accidental Escalation**

Overreliance on automation can lead to "automation complacency," where human operators trust AI outputs without verification. In high-stakes environments, this could echo incidents like the 1983 Petrov incident, where a false missile alert nearly prompted nuclear retaliation—except AI, not a human, might be at the center next time.[30] Further, if that analogy is inverted, Petrov's intervention (human intervention at large) was necessary because the early-warning technology of the time was unreliable. In theory, AI-enabled early warning systems may reduce false alarms by improving detection fidelity and data integration. However, their opacity and the potential for unpredictable failure may introduce newer forms of uncertainty—ones that may erode, rather than enhance, human confidence and oversight in moments of crisis.

- **Deliberate Escalation**

Adversaries could manipulate AI systems through disinformation or spoofed inputs, potentially engineering escalation. Alternatively, AI might be used to plan or execute precision attacks on strategic assets, such as mobile missile launchers or dual-use airbases, increasing fears of a disarming first strike.

Historical nuclear near-misses and hypothetical AI-driven scenarios illustrate how AI could exacerbate these risks.

Incident	Date	Description	Hypothetical AI-Driven Scenario	Potential AI-Related Risk
1983 Petrov Incident	Sept 26, 1983	The Soviet early-warning systems had falsely detected an incoming U.S. missile; when Lieutenant Colonel Stanislav Petrov flagged it a false alarm, in turn, averted escalation.[31]	In case of the potential involvement of an AI system here, it may possibly detect ambiguous data and flag an imminent attack, but due to brittle pattern recognition, may misclassify noise as a real strike.	A false positive trigger, and a rapid automated response as a result, possibly with minimal or even without human override, may potentially lead to accidental escalation.
1979-80 NORAD Computer Glitch	Nov 9, 1979	A faulty 46-cent computer chip had caused a false alarm of a large-scale Soviet missile attack on the U.S., which was eventually	The AI anomaly detection system may misinterpret the corrupted telemetry data from the (then) worn out chips as an actual attack and may potentially	Overreliance on AI alerts in such situations may cause operator overload and lead to potential failure in critically assessing warnings.

		dismissed after verification.[32]	trigger alerts that in turn cascade through automated defense protocols.	
1995 Norwegian Rocket Incident	Jan 25, 1995	A Russian radar had mistakenly interpreted a scientific rocket launched by American and Norwegian scientists as a possible U.S. missile attack; which was eventually quickly resolved without action.[33]	Hypothetically, AI surveillance systems may autonomously classify a scientific or commercial rocket as a hostile missile launch, and may potentially initiate automatic defensive measures.	The possibility of an automated escalation may arise due to misclassification and lack of human contextual judgment.
2022 BrahMos Missile Misfire	March 9, 2022	India accidentally launched a BrahMos cruise missile, landed in Mian Channu, Pakistan raising concerns of miscalculation during heightened tensions with Pakistan.[34]	In case of a potential involvement of AI-guided systems, mistaken identifications of a possible training or test missile as an actual enemy launch could automatically escalate alert levels or possibly trigger retaliatory actions.	Possible AI-driven misclassification and rapid automated responses may have the potential to increase risk of unintended escalation.

- **Intelligence, Targeting, and Strategic Miscalculation**

Modern AI tools enhance intelligence collection and analysis by fusing signals, imagery (GEOINT), and open-source (OSINT) data. At the strategic level, AI-driven systems are being developed to enable robust ISR (Intelligence, Surveillance, and Reconnaissance), including object identification across satellite imagery, drone feeds, and other sources. This accelerates precision targeting of strategic assets, which may blur the line between conventional and nuclear warfighting. For instance, the U.S. early-warning satellites and nuclear-capable bombers have both conventional and nuclear roles,[35] as does Russia's dual-capable Iskander missile system.[36] If AI enhances the perception and effect of a potential disarming strike, it could undermine deterrence stability and incentivize preemption.[37] The intersection of AI with both nuclear and conventional military systems, therefore, introduces a range of scenarios where escalation—whether accidental, inadvertent, or deliberate—may be triggered or intensified. As these systems evolve, the risks will not only persist but deepen, requiring urgent attention to guardrails, transparency, and human-in-the-loop safeguards.

Strategic Consequences: From False Confidence to Escalation

- **Remote Sensing and Deterrence Instability:**

AI-enhanced remote sensing could undermine strategic ambiguity by identifying the location of otherwise concealed assets (e.g., SSBNs or mobile missile launchers). As detection technologies advance across naval and aerial domains, the ability to conceal nuclear assets also diminishes. This reduction in survivability undermines second-strike credibility, which remains central to deterrence stability, and may paradoxically

increase first-strike incentives among states that fear their arsenals are vulnerable to pre-emptive attack.[38]

- **Doctrine Shifts and Escalatory Behavior:**

In response to perceived AI breakthroughs, adversaries may take destabilizing steps such as:

1. Raising alert levels of nuclear forces;
2. Automating launch protocols;
3. Adjusting doctrines to favor preemption;
4. Engaging in aggressive brinkmanship or coercive signaling;
5. Competing in a rapid AI arms race with minimal safety protocols.

These reactions are not just hypothetical; they reflect historical patterns of technological arms races and strategic misperception.

For example, on March 22, 2003, U.S. troops fired a Patriot missile at what their computer-powered system identified as an incoming Iraqi missile, but it was actually a UK Tornado fighter jet.[39] The missile struck the Tornado, killing two crew members in a tragic friendly fire incident. An RAF inquiry found the shoot-down resulted from the Patriot system's target classification error, firing rules, autonomous operation, and the Tornado not broadcasting its "friend or foe" signal.[40] The missile's manufacturers describe it as featuring automated operations with a man-in-the-loop override—enabling rapid target engagement at the speed required for missile defense missions.[41] This machine error highlights the risks of automated battlefield systems misidentifying targets. The incident demonstrates how AI can mitigate human mistakes but also introduce new, potentially dangerous errors in warfare. While automation is vital for anti-air and anti-missile systems, human operators remain indispensable in preventing accidental or erroneous engagements. Achieving the right balance between human judgment and machine decision-making, however, is inherently challenging.[42]

Stability-instability paradox

At an Operational Level: Loss of Control

AI's increasing role in adjacent military systems, surveillance platforms, decision-support tools, and autonomous operations thus introduces destabilizing dynamics that could erode the strategic logic underpinning nuclear deterrence. The impact here on the classic stability–instability paradox[43] may not therefore be through direct control of nuclear weapons, but through entangled escalation pathways, misperception, and the compression of decision time in crises shaped by AI.

This evolving convergence compounds the stability–instability paradox: [44] the idea that mutual nuclear deterrence reduces the likelihood of absolute war but may permit, and perhaps even encourage, conflict at lower levels. AI potentially exacerbates this paradox not just by accelerating warfare but also by reshaping how states perceive, respond to, and signal in crises. AI-enabled systems compress decision-making cycles, automate threat detection, and process vast amounts of data, but they also increase the risks of misperception and overconfidence.

First, AI can accelerate the pace of tactical and operational decision-making.[45] Intelligence fusion, threat detection, and predictive modeling driven by machine learning may risk compressing the "warning to response" window. This then heightens the risk of false positives or overreactions, especially under

ambiguous conditions. These systems often operate in an opaque manner, making it difficult for decision-makers to fully understand how an AI-derived conclusion was reached, thereby creating a dangerous dependency on "black box" outputs during crisis escalation scenarios.[46]

Second, in an era where strategic ambiguity and narrative warfare are central tools of deterrence, AI systems tasked with identifying adversarial intentions could misclassify deliberate ambiguity as imminent aggression.[47] For instance, when states employ deceptive signaling, such as the ambiguous deployment of dual-capable delivery platforms, cyber capabilities, and grey zone operations that blur intent, AI systems trained on historical datasets may misread deliberate ambiguity as imminent escalation.

Finally, adversarial manipulation and disinformation, which have now become hallmarks of hybrid warfare, could be used to deliberately feed false data into AI systems via spoofing, sensor saturation, or synthetic media, distorting their threat assessments.[48]In a conflict-like scenario that may be governed by AI-influenced perceptions, the possibility of inadvertent escalation becomes more likely, even in the absence of explicit nuclear moves.[49]

> "Adversarial manipulation and disinformation, which have now become hallmarks of hybrid warfare, could be used to deliberately feed false data into AI systems via spoofing, sensor saturation, or synthetic media, distorting their threat assessments. In a conflict-like scenario that may be governed by AI-influenced perceptions, the possibility of inadvertent escalation becomes more likely, even in the absence of explicit nuclear moves.

At a Structural Level: Erosion of Deterrence Foundations

Now, while these operational and perceptual risks highlight how AI could trigger inadvertent conventional escalation through loss of control or misinterpretation, the technology also poses a deeper, structural challenge to nuclear stability. Going beyond the problem of opaque outputs, AI could also undermine the very factors that sustain deterrence, such as the assured security of second-strike capabilities. By enhancing real-time surveillance, predictive targeting, and counterforce accuracy, AI may even erode confidence in the survivability of nuclear forces. Hypothetically, in scenarios where near-peer adversaries achieve technological parity while still subscribing to mutual assured destruction (MAD), this perceived fragility may lower the threshold for conventional or sub-conventional conflict, even if nuclear deterrence formally remains intact. In effect, then, AI integration simultaneously may actually erode human control while deepening the illusion of control—a paradox that links inadvertent escalation to broader structural instability.

At a Psychological & Doctrinal Level: The Stability–Instability Paradox, Brinkmanship, and the Illusion of Control

On the psychological and doctrinal plane, conversely, when states seek to accelerate decision-making and minimize human latency, AI-enabled systems may also foster a false sense of confidence in the accuracy and reliability of early warning data. This perceived precision can embolden more aggressive posturing under the belief that AI enhances control over escalation.[50] Yet, history has offered some sobering lessons: even human-led systems have produced false alarms, often narrowly averted by individual restraint. The difference with AI, however, as aforementioned, lies in its opacity and speed. In high-pressure scenarios, decision-makers may not have time to fully understand why a system flagged a threat, nor be able to interrogate the underlying logic. Faced with a time-compressed crisis, they may act on flawed, biased, or manipulated data, amplifying the risk of catastrophic miscalculation. But while AI introduces risks of inadvertent escalation, it also continues to amplify the stability-instability paradox: by creating the perception of faster, more accurate, and controllable decision-making, AI may embolden states to engage in riskier conventional or limited nuclear maneuvers, believing they can manage escalation under its guidance.

AI integration also complicates the traditional dynamics of brinkmanship.[51] Under the logic of mutual assured destruction, states have long engaged in calibrated risk-taking to signal resolve.[52] With AI, this signaling has the potential to take newer and dangerous forms, particularly in cyberspace, where attribution is murky, and escalation ladders are poorly defined. The very characteristics that make AI appealing, i.e., speed, autonomy, and predictive capability, can also obscure intent and distort perceptions. Whether this reinforces or undermines MAD depends on how states internalize these dynamics. For example, if AI heightens uncertainty and mutual vulnerability, it could strengthen deterrence; but if it fosters a false sense of control or precision, it risks eroding the very caution on which MAD depends.

“
AI integration also complicates the traditional dynamics of brinkmanship.[51] Under the logic of mutual assured destruction, states have long engaged in calibrated risk-taking to signal resolve.[52] With AI, this signaling has the potential to take newer and dangerous forms, particularly in cyberspace, where attribution is murky, and escalation ladders are poorly defined. The very characteristics that make AI appealing, i.e., speed, autonomy, and predictive capability, can also obscure intent and distort perceptions.

Critically, the destabilizing potential of AI does not require it to control nuclear launch decisions. Even partial integration into early warning, targeting, or threat detection can undermine the psychological and procedural foundations of deterrence. By clouding situational awareness and accelerating threat perception, AI shifts the calculus of nuclear stability from one based on mutual clarity to one marred by technical uncertainty. The strategic environment is thus already being reshaped, well before the full-scale integration of AI and nuclear command, control, and communications (NC3). AI need not launch warheads to unravel deterrence; it only needs to erode the assumptions, timelines, and communication channels on which nuclear stability depends.

Echoes of the Atomic Age: Parallels and Divergences

AI and Nuclear Weapons: Structural and Psychological Similarities

The rapid emergence of artificial intelligence (AI) as a transformative and potentially destabilizing technology calls for a retrospective gaze toward another epoch-defining innovation with which it is increasingly entangled, one that reshaped global security dynamics: nuclear weapons. This comparison is not just rhetorical—it is a functional and strategic imperative. Just as the dawn of the atomic age forced the international system to contend with unprecedented destructive capability, the rise of AI—particularly as it converges with military and strategic applications—demands a similarly serious reassessment of global governance mechanisms. The nuclear age provides a cautionary tale of governance delay, strategic opacity, and escalating brinkmanship; a legacy that the AI era cannot afford to replicate.

At the structural level, both nuclear technology and AI share characteristics that complicate their integration into existing international frameworks: dual-use functionality, rapid development, high strategic ambiguity, and a profound potential to upend global power equilibria. Like the fission technologies of the 20th century, AI today is a dual-use innovation—civilian in origin and intent, but with military and intelligence applications that can be deeply disruptive. Nuclear and AI technologies present a striking contrast in developmental trajectories. The nuclear bomb emerged first as a weapon—its initial use was military, not civilian—followed only later by the harnessing of atomic energy for peaceful purposes. In contrast, artificial intelligence originated in civilian contexts: academic research, commercial applications, and social computing. Yet both technologies, despite their inverse origins, share a common fate as quintessential Emerging Disruptive Technologies (EDTs): born of scientific advancement, and swiftly co-opted into the theatre of geopolitical competition. In both cases, dual-use potential has driven rapid militarization, raising strategic stakes and overwhelming governance frameworks.

> Both nuclear technology and AI share characteristics that complicate their integration into existing international frameworks: dual-use functionality, rapid development, high strategic ambiguity, and a profound potential to upend global power equilibria. Like the fission technologies of the 20th century, AI today is a dual-use innovation—civilian in origin and intent, but with military and intelligence applications that can be deeply disruptive.

Psychologically, both technologies have incited a blend of awe and anxiety. The existential dread catalyzed by nuclear weapons—epitomized by the doctrine of Mutually Assured Destruction (MAD)—finds an echo in current concerns about autonomous weapon systems, AI-led escalation, and the erosion of human agency in warfare. Both have spawned myths of omnipotence and fears of loss of control. The AI discourse today is saturated with a similar rhetoric of inevitability and inevitability-induced fatalism that characterized nuclear discussions in the Cold War: a sense that once a capability exists, its proliferation and use become foregone conclusions unless actively resisted.

Yet it is precisely this structural and psychological resonance that underscores the urgency of proactive governance. The international community failed to anticipate the rapid diffusion of nuclear capabilities post-1945; a failure that produced a world order teetering on deterrence logic and crisis management rather than enduring security. With AI, the stakes are arguably higher because the boundary between peace and war, civilian and military, decision-maker and system, is far more porous and accelerative.

Tracing the Nuclear Governance Arc

To chart a path for regulating AI integration, it is imperative to revisit the nuclear governance trajectory—each milestone, failure, and the logic that underpinned it. The atomic bombings of Hiroshima and Nagasaki in 1945 marked the genesis of a new world order. Washington's initial monopoly had given way to Soviet parity by 1949, eventually triggering an arms race that then engulfed multiple states and birthed a security paradigm that rested not on restraint, but on retaliatory capabilities.

Governance in the nuclear domain hence emerged reactively and incrementally. Subsequently, the Treaty on the Non-Proliferation of Nuclear Weapons became the cornerstone of the nuclear order, but it also institutionalized a hierarchy of nuclear "haves" and "have-nots," entrenching power asymmetries. Safeguards were eventually introduced via the IAEA, yet verification regimes still remained fragile, loophole-ridden, and subject to political manipulation. Strategic arms limitation treaties (SALT, START) and arms control measures (ABM, INF) provided some ballast, but only in the aftermath of crises—the Cuban Missile Crisis (1962), the Kargil (1999), etc, not in their anticipation.

Historical Parallels: Lessons from the Atomic Age

- **Strategic Ambiguity and Deterrence Cultures:** Nuclear weapons, over the years, have been defined by opacity, in which ambiguity in their doctrine, the existence of red lines, and command-and-control protocols have enabled a culture of deterrence and brinkmanship. AI, particularly in its military applications (autonomous systems and decision-support tools), is already replicating this strategic opacity. Nations are developing AI-enabled capabilities without clear doctrines, mirroring the uncertainty of the early Cold War. Yet unlike nuclear weapons—whose existential potential demanded explicit doctrines of use and control—AI's fungible, cross-domain character may require a doctrine of a different kind: not one that deals with its employment, but one that addresses the levels of integration, oversight, and human accountability. Both these domains, however, reveal how technological ambiguity can simultaneously deter and destabilize.

- **Governance Breakdown and Technological Overreach:** Another defining flaw of the nuclear age was the lag between innovation and regulation. Despite the IAEA's creation and arms control treaties, governance always trailed behind capability. AI is at a similar inflection point: the technology is racing ahead of normative frameworks. Yet the parallel has some limitations—nuclear governance was exceptional, focused on restriction and non-proliferation, whereas AI, as a diffuse and dual-use technology, demands a different model of governance, one that may be centered on transparency, accountability, and human oversight rather than outright prohibition. The lessons, however, stand clear that retroactive governance is fragile. The AI domain, hence, offers a brief window to apply these lessons prospectively, not reactively.

Divergences: Governance in a Decentralized Era

- **Private Players and the New Arms Race:** Unlike the nuclear age, which was largely state-driven, AI's innovation ecosystem is led by private tech companies, most of which are transnational and commercially motivated.[53] This may create a fundamental mismatch, i.e., state-level accountability versus corporate innovation. Whereas nuclear arms control negotiations back in the day were largely state-centric, AI governance now must contend with fragmented ownership, corporate secrecy, and profit-driven incentives. This risks complicating traditional approaches to regulation, transparency, and accountability.

- **Accessibility and Proliferation Risks:** Nuclear technology, though proliferated, was gated by materials, expertise, and treaty regimes. However, AI technology, by contrast, is open, accessible to the public, and rapidly diffusing. The same algorithms that power facial recognition or logistics optimization can be weaponized for autonomous targeting or surveillance. This lower barrier to entry exponentially increases horizontal proliferation risks—not just among states, but among non-state actors. While these actors may not possess nuclear weapons, their use of the said AI-enabled cyber or disinformation tools could interfere with nuclear command-and-control systems, manipulate early-warning networks, or trigger misperceptions among nuclear-armed states. AI proliferation, hence, could indirectly magnify nuclear risk by widening the range of actors capable of influencing or destabilizing nuclear decision environments. The decentralized nature of AI makes comprehensive controls far harder to enforce than in the nuclear realm.

Nuclear Successes and Failures: Applicability to AI

The nuclear governance regime also provides valuable precedents for managing high-stakes, dual-use technologies, but its applicability to AI may be uneven given the fundamental differences in technology, diffusion, and control:

Transferable Mechanisms:

- **Verification and Inspection Regimes (e.g., IAEA Safeguards)**: The IAEA's model of continuous monitoring, inspections, and transparency efforts provides a valuable framework for AI governance. This may be particularly useful in certifying compliance with agreed-upon standards for AI development and deployment in military contexts. Techniques such as audits, source code reviews, and hardware certification could be used to mimic nuclear safeguards.
- **Bilateral and Multilateral Treaties:** Although their efficacy in the present may be debatable, agreements such as SALT, START, and the NPT do illustrate the importance of formalized, legally binding commitments with verification and enforcement provisions. Similarly, potential international AI treaties could establish norms for use stages, levels of integration, data sharing, and risk reduction, especially for military AI applications.
- **Confidence-Building Measures:** Nuclear CBMs—such as hotlines, data exchanges, and transparency protocols—continue to help mitigate misperceptions and accidental escalation. Similarly, AI governance could adopt analogous measures, including sharing information on AI system capabilities, limitations, and testing procedures, to reduce uncertainty and mistrust.

Non-Transferable or Challenged Mechanisms:

- **Slow and Formalized Negotiations:** Nuclear treaties do require protracted negotiations among a limited group of stakeholders. However, given the rapid innovation cycles of AI systems and their diffusion across civilian, commercial, and military domains, attempts to craft universal, treaty-style regulation would likely prove equally slow and quickly outdated. Moreover, what exactly should be regulated also remains contested—is it the integration of AI into nuclear command-and-control? Its coupling with autonomous delivery systems? Or is it its use in strategic decision-support? As stated, unlike fissile material, these are not discrete or easily verifiable. Efficient governance measures may therefore need to focus on transparency, human oversight, and bounded autonomy rather than prohibitions. Yet defining and enforcing such thresholds may inevitably collide with issues such as a lack of political will and sovereignty concerns. This may suggest that AI governance depends less on formal treaties and more on iterative, norm-based understandings among major powers. AI's rapid innovation cycle and diverse actors necessitate more agile, adaptive governance mechanisms that can keep pace with technological change.
- **Clear Thresholds and Definitions:** Nuclear arms are defined by distinct physical characteristics and thresholds (e.g., warhead counts, yield). AI, however, lacks universally agreed-upon definitions, with intangible capabilities and risks that widely vary across domains and applications, thereby complicating the establishment of enforceable limits. While nuclear governance offers crucial lessons—particularly regarding verification, treaty-building, and confidence-building—AI's rapid development, opacity, and versatility require novel governance approaches. Future AI frameworks could blend traditional state-centric diplomacy with multistakeholder cooperation, incorporate technical auditing tools, and embrace adaptive, iterative regulation to address these challenges effectively.

Toward Smarter Governance: Avoiding the Nuclear Pitfalls

Further, the nuclear regime, while successful in averting full-scale war, has debatably suffered from three persistent deficits: opacity, exclusivity, and lag.[54] These must not be replicated in AI governance. AI's developmental arc presents an opportunity to embed norms before red lines are crossed. Unlike the nuclear past, where governance followed catastrophe or brinkmanship, AI governance can be anticipatory and inclusive—if driven by the right coalitions and frameworks. Crucially, AI's impact cuts across civilian and military domains, democratizing both innovation and risk. This underscores the need for multi-stakeholder frameworks that integrate private actors, prioritize transparency, and adopt global guardrails before crisis conditions force reactive regulation. These deficits are precisely what AI must avoid.

> The nuclear regime, while successful in averting full-scale war, has debatably suffered from three persistent deficits: opacity, exclusivity, and lag. These must not be replicated in AI governance. AI's developmental arc presents an opportunity to embed norms before red lines are crossed. Unlike the nuclear past, where governance followed catastrophe or brinkmanship, AI governance can be anticipatory and inclusive—if driven by the right coalitions and frameworks.

The nuclear governance architecture, while successful in averting full-scale war between major powers, has been widely criticized for its exclusionary design, lack of enforceability, and inability to address horizontal and vertical proliferation fully. AI, still in its relative infancy, presents a window of opportunity—however brief—to apply these lessons prospectively rather than retrospectively. Yet, unlike nuclear technology, AI's widespread accessibility, dual-use character, and rapid innovation cycle make traditional enforcement far more difficult, because the barriers to acquisition, adaptation, and misuse are far lower; this necessitates governance models that emphasize transparency, norms, and multi-stakeholder engagement rather than strict control.

Given these resonances and risks, several principles emerge from the nuclear experience that can inform AI governance.

- **Verification and Transparency:** Unlike nuclear materials, AI capabilities are intangible, reproducible, and accessible. This demands innovative verification systems, including regular auditing of algorithms, the possibility of third-party oversight, AI incident repositories, and transparent, enforceable, and resilient red-flag alert systems.
- **Anticipatory Regulation, Not Reactive Containment:** The nuclear age had demonstrated the perils of waiting for crises to spur regulation. Taking a cue from this, AI governance also needs to be anticipatory, grounded in foresight scenarios, red-teaming exercises, and multi-stakeholder consultations before a crisis unfolds. Practically, however, implementing such anticipatory governance is challenging; one cannot fully know the risks or gaps until they are encountered in real-world contexts, making proactive design inherently uncertain.
- **Multilateralism Over Exclusive Clubs:** While forums like the G7[56] and OECD[57] have made important strides in AI ethics, a truly effective regime must be inclusive and avoid the elite club model that failed to generate global legitimacy in nuclear governance. The Global South, private actors, and civil society must be integrally involved.
- **Red Lines and Norms for Autonomous Systems:** Just as chemical and biological weapons are governed by categorical bans, AI-enabled systems may also be subject to clearly articulated red lines. Autonomous nuclear command and control, lethal autonomous weapons without meaningful human control, and AI-driven escalation in nuclear postures could explicitly be prohibited under international legal instruments.

The unravelling of nuclear governance regimes offers a sobering precedent for integrating AI into military and strategic systems. Arms control fatigue, the erosion of multilateral trust, and the stagnation of treaties such as the NPT[58] and INF[59] reveal how governance frameworks can become brittle when they are slow to adapt, structurally exclusionary, or decoupled from technological realities. In the case of military-AI, the risk is not simply regulatory absence—but the entrenchment of governance models that are narrowly state-centric, technologically opaque, and shaped by a few dominant actors. While international frameworks and voluntary norms exist, they largely reflect the priorities of leading powers, tend to offer limited enforceability, and may leave emerging states and non-state actors outside oversight. These dynamics mirror the exclusivity that plagued nuclear order, where power was consolidated among a few, verification mechanisms proved limited, and emerging actors remained outside the regime.

As AI systems increasingly influence strategic decision-making, early warning networks, and potentially even nuclear-adjacent command and control architecture, the need for governance that is anticipatory, multilateral, and technologically literate becomes urgent. Without this, AI risks inheriting not only the

escalatory potential of the nuclear age, but also its governance deficiencies—marked by inertia, fragmentation, and a failure to reconcile rapid technological change with global strategic stability.

Why Governance Can't Wait

As established earlier, the strategic entanglement of AI with military systems is no longer a distant prospect—it is a present and accelerating reality. Yet, policy frameworks remain dangerously behind the curve. The pace at which AI is being integrated into nuclear-adjacent settings has far outpaced regulatory consensus. Escalation risks are intensifying not merely because of AI's technical capabilities, but because of the fragmented, reactive nature of current policy responses. Compounding this is a widening civil-military gap: the private sector continues to lead in AI innovation, while militaries adopt and deploy systems with limited transparency or alignment with broader democratic accountability. Unlike the nuclear age, where technological control was more centralized and treaty-driven, AI's diffusion is faster, more opaque, and entangled with commercial interests. The nuclear experience shows that arms control emerged not merely as a response to crises, but as a result of shared incentives: reducing the risk of catastrophic war, maintaining strategic stability, and signaling restraint to adversaries and domestic audiences alike.

The key question for AI is whether similar motivations exist—can states see value in establishing norms or regulatory frameworks that mitigate systemic risks, manage the escalation of crises, and maintain credibility, even in the absence of existential weapons? While initiatives like the REAIM summits have drawn global attention, they have yielded little substantive progress.

Without timely, anticipatory governance frameworks that include both state and non-state actors, the risk of cementing an architecture of strategic instability increases—one in which automated miscalculations, attribution ambiguity, and fragmented oversight become normalized. The longer this governance vacuum persists, the more likely it is that AI becomes embedded in security infrastructures in ways that are resistant to regulation, oversight, or rollback—replicating the very rigidity that doomed nuclear arms control.

> "Without timely, anticipatory governance frameworks that include both state and non-state actors, the risk of cementing an architecture of strategic instability increases—one in which automated miscalculations, attribution ambiguity, and fragmented oversight become normalized. The longer this governance vacuum persists, the more likely it is that AI becomes embedded in security infrastructures in ways that are resistant to regulation, oversight, or rollback—replicating the very rigidity that doomed nuclear arms control.

Proposal for an International AI Security Council

To address the risks posed by military AI entanglement, a dedicated multilateral institution, such as an International AI Security Council (IASC), could be established. This could draw from the model of the International Atomic Energy Agency (IAEA). The IASC may serve as a global platform to enhance

transparency, build trust, and ensure responsible AI governance in security-sensitive domains.

Potential Mandate for Consideration :

- **Regular Auditing of Military AI Systems:** Conduct independent audits of AI-enabled military technologies, possibly focusing on verifying adherence to the agreed-upon ethical, technical, and safety standards, including human control protocols and robustness against adversarial manipulation.
- **Monitoring of Dual-Use Technologies:** Track the development, deployment, and transfer of dual-use AI technologies that may impact strategic stability.
- **Facilitate Confidence-Building Measures:** Organize data-sharing, joint exercises, and verification mechanisms to foster transparency among member states and reduce misperceptions and escalation risks.
- **Research and Norm Development:** Collaborate with academia, industry, and civil society to develop best practices, technical norms, and verification methodologies for military AI.
- **Incident Investigation:** Act as an impartial body to survey AI-related security incidents or near-misses that risk escalation, providing a platform for unbiased assessments and recommendations.

Possible Membership Scenarios:

- The IASC would need to be inclusive and globally representative, explicitly incorporating voices from the Global South, emerging AI powers, and nuclear and non-nuclear states alike.
- Membership criteria would balance expertise, technological capability, and geopolitical diversity to foster legitimacy and broad buy-in.
- It would operate on principles of transparency, accountability, and cooperation, with voting rights and decision-making processes designed to avoid veto deadlocks while respecting state sovereignty.

Strategic Rationale and Hypothetical Incentives:

Institutionalizing AI security governance through the IASC would provide several strategic and systemic benefits:

- **Preventing Destabilizing Arms Races:** By promoting transparency and information-sharing, the IASC could help slow a potential spiral of weaponization in autonomous and algorithmic warfare systems.
- **Empowering Emerging States:** Inclusion of the Global South could help democratize norm-setting and prevent AI governance from becoming another arena of technological dependency or exclusion.
- **Bridging the Trust Deficit:** A neutral, rules-based forum would create much-needed channels for dialogue between major powers that currently lack shared guardrails on AI use in military operations.
- **Enhancing Crisis Stability:** Through incident reporting and redressal mechanisms, the IASC may mitigate the risk of accidental or inadvertent escalation in regions with fragile deterrence dynamics.

By institutionalizing AI security governance in this manner, an IASC-like body may help prevent destabilizing arms races, promote ethical AI use in the military, and provide a framework for international cooperation that is both equitable and effective. Much as the IAEA anchored nuclear stability during the atomic age, the IASC (or a similar body) could emerge as the central institution of AI-era strategic stability, ensuring that technological progress reinforces rather than undermines international peace and security.

A Policy Answer for a Technical Problem:[60] Strategic Technology, Strategic Governance

The nuclear age, hence, provides both a warning and a blueprint. It teaches that rapidly advancing technologies can destabilize the international order if governance lags behind—and that competition can corrode trust even among rational actors. It also reveals how scientific breakthroughs, once militarized, can provoke decades-long standoffs in the absence of robust regulatory intervention.
Yet, the same history also shows that regulation may not be too far-fetched. Treaties, doctrines, and verification regimes—however imperfect—had emerged through a mix of political will, civil society pressure, and institutional adaptation. The AI era has not yet crossed the same point of no return. There remains a crucial window to apply foresight, coordination, and normative constraints before governance becomes reactive and crisis-driven. The challenge is not in the absence of precedent—but in the will to act before a catastrophe.

These global dynamics are not abstract; they manifest differently across national contexts, depending on each state's strategic environment, technological capacity, and institutional culture. Among them, India's experience stands out as a particularly revealing case.

The Indian Case Study

The Indian Imperative: Between Restraint and Relevance

Despite the risks and regulatory imperatives discussed earlier, states will continue to integrate AI into their military and nuclear-adjacent systems. The drive toward perceived deterrence advantages makes this trajectory effectively irreversible. Regulation may therefore not begin from an assumption of abstention or rollback but rather stem from a realistic understanding of why states pursue such integration in the first place, and how they might perceive its benefits, vulnerabilities, and strategic value. Effective AI governance must engage with this logic rather than deny it, aligning risk-reduction mechanisms with state incentives rather than against them.

Within this context, as global debates on military AI governance often unfold in the abstract, for states like India, these questions may be inseparable from their immediate security realities. For instance, India's strategic environment is defined by a rapidly evolving regional threat landscape and an already accelerating global AI arms race. As China operationalizes its doctrine of "intelligentized warfare"[61] and deepens its military-technical collaboration with Pakistan,[62] New Delhi faces mounting pressure to ensure that its deterrent posture remains credible in both conventional and nuclear domains. India, hence, stands at a crossroads—much like it did during the early nuclear age. Here, from the state's perspective, the choices it makes now will determine not only the country's technological sovereignty but also its strategic autonomy. The stakes are high: falling behind in AI today could compromise both national security and economic competitiveness tomorrow. Yet, such an imperative for technological advancement must be balanced with an equally urgent need for responsibility.

Calls, therefore, for robust governance of military AI—especially where it intersects with nuclear command and control—must not be misconstrued as arguments for technological abstention. Governance and capability are not mutually exclusive; in fact, one may be ineffective without the other.

Strategic prudence demands that India accelerate its military AI development—not recklessly, but deliberately, anchored in democratic accountability and ethical principles. Normative leadership is most persuasive when backed by technical capacity. To shape global AI governance regimes and prevent destabilizing asymmetries in the region, India must be a critical actor. For India, the challenge may not be whether to develop military AI, but how to do so while preserving strategic stability and minimizing systemic risk—the very concerns this report has outlined at the global level.

From this perspective, India's task is twofold: to develop AI capabilities that secure its strategic interests, and simultaneously to embed those capabilities within transparent, accountable, and norm-sensitive frameworks. In doing so, India can bridge the growing divide between capability development and governance design—a divide that has hampered global debates on AI stability.

Unlike the nuclear era, the window for strategic advantage in AI is not just closing quickly—it may never reopen. But unlike the nuclear experience, this moment also offers the possibility of globally shaping governance before catastrophe, not after it. India's engagement, therefore, must combine technological ambition with anticipatory regulation, ensuring that innovation serves stability rather than undermines it.

South Asia's Regional AI Threat Landscape

As aforementioned, the strategic environment of India is also increasingly defined by the rapid, AI-driven military modernization of its two primary regional competitors: China and Pakistan. Both countries are integrating AI capabilities that pose multifaceted challenges to India's nuclear and conventional deterrence postures. The nature of these developments may be characterized as nuclear-adjacent risks, insofar as the integration of AI into surveillance, command, and decision-support architectures has direct implications for deterrence stability and the credibility of nuclear command and control systems.

> China and Pakistan are integrating AI capabilities that pose multifaceted challenges to India's nuclear and conventional deterrence postures. The nature of these developments may be characterized as nuclear-adjacent risks, insofar as the integration of AI into surveillance, command, and decision-support architectures has direct implications for deterrence stability.

China's AI Advancements and "Intelligentized Warfare" Doctrine

China's 2019 Defense White Paper[63] explicitly underlines the centrality of AI and autonomous systems to its military modernization, emphasizing a transition toward "intelligentized warfare" that integrates AI across ISR, command and control, and precision strike domains. China's deployment of AI-driven ISR platforms—including advanced satellites, drones, and electronic warfare systems—significantly enhances its ability to conduct real-time battlefield awareness and targeting against Indian forces. The PLA's focus on AI-enabled decision-support tools also raises the stakes for India's nuclear command and control integrity, as China may seek to compress decision timelines, potentially increasing risks of miscalculation or inadvertent conventional escalation.

Pakistan's Drone and AI-Enabled Capabilities

Similarly, Pakistan has pursued AI-enhanced military programs, albeit at a different scale and scope. Its expanding use of drones for surveillance and tactical strikes along the Line of Control and beyond demonstrates a practical application of AI-enabled autonomy in conventional conflict. Furthermore, Pakistan's ongoing military-technical cooperation with China facilitates access to emerging AI tools, which could augment Pakistan's early warning and rapid response systems. These developments complicate India's deterrence calculus, as Pakistan's asymmetric adoption of AI technologies could undermine India's conventional superiority and raise the risk of escalatory spirals in crises.

Implications for India's Deterrence and Strategic Posture

Together, China's and Pakistan's AI-driven military capabilities erode traditional benchmarks of Indian deterrence. Faster, AI-enhanced ISR and decision-making reduce reaction times and increase the pressure on India's command structures to respond effectively in the face of uncertainty. This dynamic amplifies the need for India to accelerate its own military AI integration—not only to maintain credible deterrence but also to ensure resilience against AI-enabled surprise or deception operations. India's strategic response must include investments in AI-driven ISR, robust cyber defenses, and autonomous systems, all anchored in transparent doctrines and ethical frameworks to sustain both domestic legitimacy and international credibility.

In sum, addressing these challenges requires a calibrated approach that balances capability development with governance commitments, positioning India as both a regional stabilizer and a responsible global actor in the emerging AI-military nexus.

Nuclear Timidity: Learning from the Past Precedents

In the aftermath of Hiroshima and Nagasaki, and through the early years of the Cold War, India's nuclear policy was shaped as much by restraint as by strategic ambiguity.[64] India's foundational leaders were deeply invested in projecting a morally upright, disarmament-oriented position rooted in Gandhian ideals.[65] Despite Nehru's patronage of science and his support for Homi Bhabha's ambitious atomic program,[66] India stopped short of decisively integrating nuclear weapons into its strategic calculus—until the 1962 Sino-Indian War forced a reevaluation.[67]

The costs of this ambivalence were steep. While India possessed the technical capability to develop nuclear weapons, it remained committed to vague notions of nuclear exceptionalism[68]—"keeping the bomb option open"[69] without a clear doctrinal path. The reluctance to cross the nuclear threshold stemmed from both political idealism and institutional caution, a dynamic that delayed not only strategic clarity but also technological preparedness for the country. When India finally tested nuclear weapons in 1998, it did so under duress and in defiance of a global

> Realistically, as AI becomes increasingly embedded in strategic and deterrence architectures worldwide, complete abstention is neither feasible nor prudent. India must therefore avoid excessive timidity—keeping pace with global integration of AI into nuclear-adjacent systems—while shaping robust regulatory frameworks to manage the attendant risks.

non-proliferation regime that had effectively closed ranks.

This belated assertion of nuclear capability was not just about deterrence—it was a struggle to reclaim geopolitical relevance. Yet, by then, the costs of delayed decision-making had already accumulated: constrained access to global nuclear markets, sanctions, technology denial regimes, and the absence of a robust domestic ecosystem that could have matured alongside the nuclear powers of the day.

Even more problematic was the exclusion of private enterprise from the nuclear (civilian) domain.[70] Driven by fears of monopolization and external control, India adopted a statist approach to nuclear infrastructure, concentrating authority in a handful of public-sector entities. This choice stifled innovation and scalability, outcomes that haunt India's civil nuclear program to this day. Realistically, as AI becomes increasingly embedded in strategic and deterrence architectures worldwide, complete abstention is neither feasible nor prudent. India must therefore avoid excessive timidity—keeping pace with global integration of AI into nuclear-adjacent systems—while simultaneously and more importantly shaping robust regulatory and ethical frameworks to manage the attendant risks.

Avoiding the Nuclear Déjà Vu: A Parallel in the Age of AI?

India's approach to AI today carries uncomfortable echoes of its early nuclear trajectory. As the world races ahead in the development and deployment of AI—particularly in the military and strategic sectors—India risks repeating its past errors: lack of strategic clarity, and excessive centralization. Here, strategic clarity would entail a defined national doctrine articulating how AI fits within India's defense posture, deterrence strategy, and broader governance approach. And while centralization may mitigate proliferation risks, India's excessive centralization—within this report's reasoning—hampers innovation, inter-agency coordination, and adaptive capacity, thereby undermining the very strategic competitiveness it seeks to preserve.

Much like nuclear energy, AI is a quintessential dual-use technology—civilian in its origins but increasingly militarized in practice. From battlefield autonomy to intelligence processing, from cyber defense to drone warfare, AI is being rapidly integrated into security infrastructures around the world. Yet India's approach remains fragmented. Government documents such as the National Strategy for AI[71] and the Defense AI Council[72] have signaled intent, but operational frameworks remain underdeveloped. There is no clear doctrine for the strategic use of AI in defense, or a roadmap for ethical AI deployment, and limited synergy between public institutions and private innovators. Paradoxically, this very fragmentation—borne of bureaucratic inertia and cautious governance—may temporarily reduce the risk of premature or unsafe AI integration into nuclear or command systems,

> "India's approach remains fragmented. Government documents such as the National Strategy for AI[71] and the Defense AI Council[72] have signaled intent, but operational frameworks remain underdeveloped. There is no clear doctrine for the strategic use of AI in defense, or a roadmap for ethical AI deployment, and limited synergy between public institutions and private innovators. Paradoxically, this very fragmentation may temporarily reduce the risk of premature or unsafe AI integration into nuclear or command systems.

even as it constrains India's long-term strategic competitiveness.

India's military, while rhetorically committed to AI modernization, lacks the institutional agility to adapt to rapid technological change. At the same time, the private sector—India's most dynamic source of AI innovation—had long been kept at arm's length from sensitive defense applications. Bureaucratic caution, regulatory opacity, and outdated procurement models continue to restrict collaboration, mirroring the public-sector gatekeeping that once throttled the growth of India's nuclear program. While such caution may indeed be perceived as sound policy for nuclear stability, the critique, however, stems from a broader concern that India's overcautious stance, while risk-averse in the short term, may erode its long-term strategic autonomy and capacity to shape global AI norms.

Catching up: Strategic Delay in an Accelerating Race?

The global AI arms race is already underway, with the United States, China, and, increasingly, Russia investing billions in integrating AI into national defense. From Pentagon initiatives like Project Maven[73] and the Joint Artificial Intelligence Center (JAIC),[74] to China's fusion of civil and military research under its AI Development Plan,[75,] great powers are not merely experimenting with AI—they are institutionalizing it.

India, by contrast, again is at risk of strategic delay. The belief that a cautious or non-aligned approach will yield long-term dividends ignores the reality that AI, unlike nuclear weapons, does not lend itself to strategic ambiguity.[76] Technological first-mover advantages in AI compound over time, through data accumulation, model refinement, and infrastructure build-out. Waiting until global norms emerge—or until others set the rules—could relegate India to a position of reactive dependence, where it merely adopts or adapts technologies created elsewhere, under terms defined by others.

Moreover, India's reluctance to explicitly prioritize military AI until after the 2025 conflict with Pakistan also undercut its ability to shape global norms.[77] Just as it advocated for disarmament without possessing strategic parity during the nuclear era, India risks entering the AI governance debate from a position of weakness. Norm entrepreneurship requires capability. Without a credible AI military capacity, India's calls for ethical AI, transparency, or equitable access will carry limited geopolitical weight.

A Technological Consciousness Gap

Underlying all of this is a deeper issue: India still lacks a coherent "technology consciousness" in national strategy.[78] Decisions on emerging technologies are often reactive and framed through the lens of regulatory compliance or moral anxiety, rather than as core components of national power. AI, like nuclear before it, is treated as an adjunct—not a driver—of strategic thinking.

India's strengths, such as a robust startup ecosystem, a globally competitive IT sector, deep pools of engineering talent, and massive data sets from its digital public infrastructure, require coordinated mobilization. To add to this, strategic foresight, institutional reform, and above all, political will, are needed to move from potential to posture.

India's AI ecosystem:

India's AI ecosystem is marked by vibrant private-sector innovation, particularly in hubs like Bengaluru, Hyderabad, and Gurugram, where hundreds of AI startups are pioneering advances in machine learning,

natural language processing, and computer vision. Companies such as Arya.ai, [79] SigTuple, [80], and Niramai exemplify India's capacity to develop cutting-edge AI applications with both commercial and societal impact. Additionally, India's large IT services firms—Infosys, TCS, and Wipro—are increasingly embedding AI capabilities into their global delivery models, demonstrating their competitive strengths.[81] However, critical gaps remain, notably a heavy reliance on foreign hardware, including GPUs and specialized AI chips predominantly sourced from the U.S. and China, which exposes India's AI ambitions to supply chain vulnerabilities and geopolitical risks.

On the military front, India faces challenges in integrating AI into defense systems due to limited indigenous grassroots AI-focused R&D within the armed forces and insufficient collaboration with private innovators, constraining the development of AI-enabled ISR, autonomous platforms, and command-and-control enhancements critical for modern warfare. To bridge these gaps, India must cultivate deeper public-private partnerships that leverage the agility and innovation of startups alongside state-backed research institutions and defense agencies. Models such as joint AI innovation hubs focused on defense applications, co-funded research consortia, and government-backed accelerator programs can incentivize indigenous hardware development, facilitate secure data-sharing agreements, and align AI R&D with strategic military priorities—transforming fragmented potential into a coherent technological posture that supports both national security and economic competitiveness.

Building a Proactive Governance Model

To correct course, India must pursue two tracks simultaneously: accelerate domestic AI capability—especially in defense—and lead global advocacy to articulate norms and principles for responsible AI use. The latter should not be seen as a soft or secondary objective. Governance is becoming a theatre of strategic competition in its own right.

Unlike nuclear governance, which was dominated by treaty-based structures and centralized state actors, AI governance will be multipolar, networked, and deeply influenced by private corporations. India's opportunity lies in helping to design flexible, inclusive models that avoid the rigidity and exclusivity that ultimately undermined the Nuclear Non-Proliferation Treaty (NPT) and similar frameworks.

India can and must push for global AI norms that:

- Acknowledge asymmetries between data-rich and data-poor nations;
- Incorporate both civilian and military applications in governance discussions.
- Promote explainability, accountability, and auditability in AI systems;
- Guard against AI-enhanced information warfare and attribution ambiguity;
- Resist the monopolization of foundational models by a handful of global players.

From Doctrine to Deployment

Domestically, this would require an overhaul of how India approaches emerging technologies. The Ministry of Defence must adopt a clear doctrine for AI integration, backed by institutional mechanisms that enable agile procurement, sandboxed experimentation, and collaboration with the private sector. Civil-military technology cooperation must be seen not as a risk, but as a requirement. Regulatory barriers must be replaced by regulatory enablers.

The defense establishment must also think beyond platforms and systems. AI in defense is not only about autonomous drones or surveillance software—it is about redefining the speed, scale, and nature of decision-making. India's armed forces must prepare for adversaries that may deploy AI to disrupt, deceive, or escalate—often below the threshold of conventional warfare. Building indigenous technological capacity must therefore proceed alongside the creation of strong governance frameworks, ensuring that agility does not come at the cost of accountability. Without indigenous capacity to respond in kind, India risks strategic obsolescence.

None of this suggests that ethical concerns should be sidelined. On the contrary, India's tradition of normative leadership—rooted in democratic values and constitutionalism—must be leveraged to ensure that AI development remains aligned with human rights and international law. But ethical anchoring must not translate into strategic paralysis. The task is to balance restraint with relevance—to lead not just by example, but by capability.

India's Military AI Integration Roadmap

Despite making strides in articulating AI's strategic importance, i.e., issuing documents such as NITI Aayog's National Strategy on Artificial Intelligence [82] and facilitating emerging initiatives within the Ministry of Defence (MoD) focused on AI-enabled defense capabilities,[83] India faces significant barriers that curb effective implementation. Procurement processes remain cumbersome and ill-suited to the fast-paced nature of AI innovation, delaying the fielding of critical technologies. For example, the MoD's AI programs have been generally hampered by bureaucratic inertia, fragmented agency coordination, and a lack of dedicated funding streams, hindering sustained R&D and prototype development. Similarly, while NITI Aayog's strategy has a comprehensive vision across many sectors, it continues to lack explicit mechanisms to ensure the translation of policy into defense-specific outcomes, especially in areas that require rapid technological adoption and integration with existing military infrastructure.

To overcome these challenges, India could consider dedicated AI defense budgets to ensure continuous, predictable funding for military AI projects, enabling long-term planning and experimentation. Enhanced inter-agency coordination-perhaps under a centralized AI Defense Innovation Unit of sorts – may be crucial for aligning objectives and pooling expertise. Additionally, streamlining procurement protocols through fast-track clearance paths and flexible contracting with startups and private firms could also accelerate capability deployment. Finally, fostering a culture of agility and risk-taking within the defense bureaucracy can help India keep pace with the evolving AI landscape, ensuring that policy ambitions translate into operational realities.\

India's approach must balance strategic capability with governance, regulation, and risk reduction. These recommendations embed safeguards into development, ensuring that India is not left behind technologically while contributing to regional stability.

To align strategic capability with responsible governance, India must move on three timelines:

Short-Term (1–2 years): Establish Foundations for Capability and Governance

- **Mapping Nuclear Adjacent AI Systems:** Begin by identifying dual-use technologies and nuclear-adjacent applications, such as ISR, early warning, and command and control, to assess escalation, misperception, and structural risks.

- **Codify Human Oversight:** Make human-in-the-loop mandatory, if possible, for all AI-enabled systems capable of impacting nuclear or strategic decisions.
- **Undertaking Internal Red-Teaming & Risk Audits:** Establish and institutionalize independent adversarial testing of military AI systems to anticipate escalation risks, and data.
- **Engaging Multi-Stakeholder Expertise:** Involving academia, industry, and civil society in auditing dual-use AI deployments will ensure that such deployments are more transparent and accountable, with ethical design. Subsequently, its mandate should be expanded to function like the U.S. Defense Innovation Unit-linking prioritized defense needs with Indian startups, ISRO, academia, and private R&D for dual-use innovation.

Medium-Term (3–5 years): Build Crisis Resilience and Regional Norms

- **Simulate Nuclear-Adjacent Escalation Scenarios:** Create controlled wargaming exercises and crisis simulations to train decision-makers to manage AI-driven misperception, compressed timelines, and autonomous system interactions.
- **Formalize Regional and Multilateral Dialogues:** Initiate AI risk-reduction dialogues with regional powers and Quad+ partners, situating India as a norm-setter in responsible military AI use in the Indo-Pacific.
- **Standardize Transparency and Audit Protocols:** Implement explainability, data provenance, and reporting standards for AI systems affecting strategic or nuclear forces, ensuring regulatory compliance aligns with operational development.

Long-Term (5–10 years): Institutionalize Governance and Strategic Leadership

- **Civil-Military AI Governance Commission:** Establish a statutory body that includes representation from defense (DRDO, MEA), technical institutions, diplomacy, academia, and industry, which would play a constructive role in overseeing nuclear-adjacent AI development, operational use, and ethical compliance.
- **Verification and Confidence-Building Measures:** Collaborate internationally to verify AI capability, data integrity, and compliance with risk-reduction measures that enhance mutual stability.
- **Integrate Governance into Strategic Doctrine:** Embed AI oversight, ethical safeguards, and nuclear-adjacent risk mitigation into India's strategic and nuclear posture, to make sure development underpins deterrence credibility while minimizing the potential for unintended escalation.

This integrated roadmap reflects the report's dual emphasis: the first half's call for international regulation and risk reduction, and the pragmatic reality that AI military integration is unavoidable. By aligning capability development with governance, India can advance its strategic interests while contributing to regional and global stability, thereby reducing the high nuclear-adjacent risks identified in the first half of the report. Developing an AI roadmap grounded in Indian realities—bureaucratic, industrial, and regional- will enable India to move from aspirational policymaking to credible capability-building. Doing so will not only enhance deterrence and operational efficiency but also enable India to play a leadership role in shaping responsible military AI norms across the Global South and the Indo-Pacific.

Governance Lessons from the Nuclear Age

Translating Cold War–era models to the digital age is not straightforward.[84] The nuclear era offers sobering lessons for AI: namely, that delayed governance, exclusive regimes, and moralistic inaction often result in greater instability, not less. As AI becomes entangled with military systems, especially those adjacent to nuclear command-and-control architectures, it is critical to draw on proven risk-reduction mechanisms from the nuclear domain.

India's emerging AI governance approach—balancing strategic autonomy with pragmatic multilateral engagement—could serve as a useful template for other middle powers that face similar constraints. Such states often operate under resource constraints, depend on foreign technology providers, and have limited leverage to shape hard-security norms. By emphasizing layered governance—domestic oversight frameworks, participation in plurilateral forums, and selective alignment with great-power initiatives—India could demonstrate how middle powers can safeguard national interests while contributing to global rule-making. In the AI-nuclear nexus, this model offers a pathway for states to mitigate risks, build verification capacity through partnerships, and push for equitable governance structures that avoid replicating the exclusivity and technology gatekeeping as seen in the nuclear era.

Key Lessons at Large

In the absence of a treaty-based architecture for AI, the burden falls on national doctrines, multilateral mechanisms, and normative leadership.

Lessons for AI governance in the military context.[85]

- **Human-in-the-Loop as a Norm:**

AI must augment, not replace, human judgment—especially in decisions involving the use of force. The international community should establish this as a minimum global standard, particularly in contexts such as lethal autonomous weapons systems (LAWS) and nuclear-adjacent platforms.

- **Crisis Management & Escalation Protocols:**

Nations should collaborate to develop AI-specific crisis management protocols that cover how to interpret and respond to unintended AI behaviors, misattributed cyber operations, or escalatory dynamics caused by algorithmic misjudgments. These measures are essential for preventing accidental conflict and maintaining strategic stability.

- **Transparency and Explainability:**

Black-box algorithms used in national security contexts must be subject to internal oversight, external auditability, and, where feasible, verifiable international norms—similar to mechanisms used in nuclear verification regimes. This enhances accountability and reduces the risk of miscalculation.

- **International Coordination on Dual-Use AI:**

There is an urgent need for a multilateral mechanism to monitor and govern the military applications of dual-use AI technologies. Such a framework could draw inspiration from existing arms control regimes, such as IAEA safeguards or the MTCR, but would need to be adapted to address the unique challenges posed by software, data, and machine learning models.

Endnotes

1. Araya, D., & King, M. (2022, March 7). The impact of artificial intelligence on military defence and security (CIGI Paper No. 263). Centre for International Governance Innovation. https://www.cigionline.org/static/documents/no.263.pdf
2. Simmons-Edler, R., Badman, R., Longpre, S., & Rajan, K. (2024). AI-Powered Autonomous Weapons Risk Geopolitical Instability and Threaten AI Research [Preprint]. arXiv. https://arxiv.org/abs/2405.01859v1
3. Johnson, J. (2022). Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decisionmaking in the digital age. Defence Studies, 23(1), 43–67. https://doi.org/10.1080/14702436.2022.2102486
4. Z Shirshikova, (2022) Comparative Analysis of the U.S.–China Artificial Intelligence Architecture and Effects of Autonomous UAVs on the Future of the Battlefield, https://dash.harvard.edu/server/api/core/bitstreams/3f854ae9-a386-4953-8b2e-d2686cb92ab6/content
5. Lax, E. (2024, August 4). The Strategic Implications of AI in Defense: Redefining the Future of Global Security. TRENDS Research & Advisory. https://trendsresearch.org/insight/the-strategic-implications-of-ai-in-defense-redefining-the-future-of-global-security/
6. Mishra, S., & Reiner, P. (2025, September 10). Artificial Intelligence in Nuclear Command, Control & Communications: A Technical Primer. Institute for Security and Technology. https://securityandtechnology.org/wp-content/uploads/2025/09/Artificial-Intelligence-in-Nuclear-Command-Control-Communications.pdf
7. Here, while these functions have been applied across both civil and military nuclear domains, applications like operator training are predominantly associated with civil nuclear facilities. This section primarily concerns military nuclear systems and NC3 operations.
8. Ibid.
9. Saab, B. Y., & White, D. D. (2025, July 16). Lessons Observed from the War Between Israel and Iran. War on the Rocks. https://warontherocks.com/2025/07/lessons-observed-from-the-war-between-israel-and-iran/ For details on the Lavender system also see, Human Rights Watch. (2024, September 10). Questions and answers: Israeli military's use of digital tools in Gaza. Human Rights Watch. https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza
10. Bondar, K. (2025, March 6). Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare
11. Euronews. (2025, June 18). Israel's spy agency used AI and smuggled-in drones to prepare attack on Iran, sources say.Euronews. https://www.euronews.com/next/2025/06/18/israels-spy-agency-used-ai-and-smuggled-in-drones-to-prepare-attack-on-iran-sources-say
12. Johnson, J. (2022). Inadvertent Escalation in the Age of Intelligence Machines: A New Model for Nuclear Risk in the Digital Age. European Journal of International Security, 7(3), 337–359. https://doi.org/10.1017/eis.2021.23
13. Kaplow, J. M., & Musto, R. A. (2025). Artificial Intelligence and the Future of Nuclear Weapons. In P. Hacker (Ed.), Oxford Intersections: AI in Society. Oxford University Press. https://doi.org/10.1093/9780198945215.003.0090
14. Kahl, C. H., & Mitre, J. (2025, July 9). The Real AI Race: America Needs More Than Innovation to Compete With China.Foreign Affairs. https://www.foreignaffairs.com/united-states/real-ai-race
15. Abraham, Y. (2024, April 3). 'Lavender': the AI machine directing Israel's bombing spree in Gaza. +972 Magazine.
16. Davies, H., McKernan, B., & Sabbagh, D. (2023, December 1). 'The Gospel': how Israel uses AI to select bombing targets in Gaza. The Guardian. https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets-in-gaza
17. Stokel-Walker, C. (2024, May 15). A new Red Cross report says AI introduces risk of 'unaccountable errors' in warfare.Fast Company. https://www.fastcompany.com/91124847/red-cross-report-ai-warfare
18. Chernavskikh, V., & Palayer, J. (2025, June). Impact of Military Artificial Intelligence on Nuclear Escalation Risk (SIPRI Insights on Peace and Security No. 2025/06). Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2025-06/2025_6_ai_and_nuclear_risk.pdf
19. Lin, H. (2025, June). Artificial Intelligence and Nuclear Weapons: A Commonsense Approach to Understanding Costs and Benefits. Texas National Security Review, 8(3), 98–109. https://doi.org/10.26153/tsw/60739
20. Future of Life Institute. (2023, July). AI and Nuclear Command, Control & Communications: A Policy Primer. https://futureoflife.org/wp-content/uploads/2023/07/FLI_AI_NC3_Policy_Primer.pdf

Endnotes

21. Reiner, P., & Wehsener, A. (2019, November 4). The real value of artificial intelligence in nuclear command and control. War on the Rocks. https://warontherocks.com/2019/11/the-real-value-of-artificial-intelligence-in-nuclear-command-and-control/
22. Chernavskikh, V., & Palayer, J. (2025, June). Impact of Military Artificial Intelligence on Nuclear Escalation Risk (SIPRI Insights on Peace and Security No. 2025/06). Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2025-06/2025_6_ai_and_nuclear_risk.pdf
23. Department of Defence Production, Ministry of Defence, Government of India. (2022). Artificial Intelligence in Defence[PDF]. https://www.ddpmod.gov.in/sites/default/files/2023-11/ai.pdf
24. Cheney-Peters, S. (2013, February 12). A Relay Race: Communication Relay Drones. Center for International Maritime Security. https://cimsec.org/communication-relay-drones/
25. Rashid, A. B., Kausik, A. K., Sunny, A. A. H., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. International Journal of Intelligent Systems. Advance online publication. https://doi.org/10.1155/2023/8676366
26. Siu, T. L. (2022, May). Autonomous Nuclear Torpedoes Usher in a Dangerous Future. U.S. Naval Institute Proceedings. https://www.usni.org/magazines/proceedings/2022/may/autonomous-nuclear-torpedoes-usher-dangerous-future
27. Saalman, L., (Eds.). (2019, October). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume II: East Asian Perspectives. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2019-10/the_impact_of_artificial_intelligence_on_strategic_stability_and_nuclear_risk_volume_ii.pdf
28. Aguirre, A., Javorsky, E., & Tegmark, M. (2023, July 17). 'Artificial Escalation': Imagining the future of nuclear risk.The Bulletin of the Atomic Scientists. https://thebulletin.org/2023/07/artificial-escalation-imagining-the-future-of-nuclear-risk/
29. United Nations. (2024, July 1). Lethal autonomous weapons systems: Report of the Secretary-General(Document A/79/88).https://docs.un.org/en/A/79/88
30. Boulanin, V., Saalman, L., Topychkanov, P., Su, F., & Peldán Carlsson, M. (2020, June). Artificial Intelligence, Strategic Stability and Nuclear Risk. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf
31. Aksenov, P. (2013, September 26). Stanislav Petrov, the man who may have saved the world. BBC News. https://www.bbc.com/news/world-europe-24280831
32. National Security Archive. (2020, March 16). False warnings of Soviet missile attacks during 1979-1980 put U.S. forces on alert.https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2020-03-16/false-warnings-soviet-missile-attacks-during-1979-80-led-alert-actions-us-strategic-forces
33. A Close Call – How Close Did We Come? FRONTLINE. https://www.pbs.org/wgbh/pages/frontline/shows/russia/closecall/
34. Aksenov, P. (2022, August 4). Stanislav Petrov, the man who may have saved the world. BBC News. https://www.bbc.com/news/world-asia-india-60711653
35. Tannenwald, N., Acton, J. M., & Vaynman, J. (Eds.). (2018). Meeting the Challenges of the New Nuclear Age: Emerging Risks and Declining Norms in the Age of Technological Innovation and Changing Nuclear Doctrines. American Academy of Arts & Sciences. https://www.amacad.org/publication/emerging-risks-declining-norms/section/4
36. https://www.iiss.org/online-analysis/online-analysis/2024/02/russias-nuclear-capable-missiles-a-question-of-escalation-control/
37. Chernavskikh, V., & Palayer, J. (2025, June). Impact of Military Artificial Intelligence on Nuclear Escalation Risk (SIPRI Insights on Peace and Security No. 2025/06). Stockholm International Peace Research Institute (SIPRI)https://www.sipri.org/sites/default/files/2025-06/2025_6_ai_and_nuclear_risk.pdf
38. Topychkanov, P. (Ed.). (2020, April). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume III — South Asian Perspectives. Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2020-04/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov_1.pdf

Endnotes

39. Atherton, K. (2022, May 6). Understanding the errors introduced by military AI applications. Brookings Institution. https://www.brookings.edu/articles/understanding-the-errors-introduced-by-military-ai-applications/
40. Ministry of Defence, U.K. (2003, March 23). Military aircraft accident summary: Aircraft accident to RAF Tornado GR MK4A ZG710(MAAS 03-02). GOV.UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/82817/maas03_02_tornado_zg710_22mar03.pdf
41. Raytheon Technologies. (n.d.). Patriot — Global Patriot® air and missile defense system. Archived webpage. Retrieved from https://web.archive.org/web/20050826224850/http://www.raytheon.com/products/patriot/ via Atherton, K. (2022, May 6). Understanding the errors introduced by military AI applications. Brookings Institution. https://www.brookings.edu/articles/understanding-the-errors-introduced-by-military-ai-applications/
42. Atherton, K. (2022, May 6). Understanding the errors introduced by military AI applications. Brookings Institution. https://www.brookings.edu/articles/understanding-the-errors-introduced-by-military-ai-applications/
43. Johnson, J. (2024). Revisiting the 'stability–instability paradox' in AI-enabled warfare: A modern-day Promethean tragedy under the nuclear shadow? Review of International Studies. Advance online publication. https://doi.org/10.1017/S0260210524000767
44. Krepon, M. (2005). The Stability-Instability Paradox in South Asia. The Asia Dialogue. https://theasiadialogue.com/wp-content/uploads/2017/10/stability-instability-paradox-south-asia.pdf
45. Erskine, T., & Miller, S. E. (2024). AI and the decision to go to war: Future risks and opportunities. Australian Journal of International Affairs.https://doi.org/10.1080/10357718.2024.2349598
46. Chernavskikh, V. (2024, September). Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities (SIPRI Background Paper, No. BP 2409). Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2024-09/bp_2409_ai-nuclear.pdf
47. Haughey, Orla. "Fake News, Real Missiles: The Potentially Disruptive Role of AI in Nuclear Decision-Making." Uttryck Magazine, 28 April 2025. https://www.uttryckmagazine.com/2025/04/28/ai-in-nuclear-decision-making/
48. Siman, Bernard. "AI And Microtargeting Disinformation As A Security Threat To The Protection Of International Forces." The Defence Horizon Journal, 23 May 2024. https://tdhj.org/blog/post/ai-disinformation-security
49. Pardo de Santayana, José. Artificial intelligence and the war in Ukraine. Instituto Español de Estudios Estratégicos / Ministerio de Defensa, December 17, 2024. "Originally published in: Artificial intelligence in geopolitics and conflicts," June 2024. https://www.defensa.gob.es/documents/2073105/2278118/la_inteligencia_artificial_y_la_guerra_de_ucrania_2024_dieeea81_eng.pdf
50. Bode, Ingvild & Watts, Tom. "Worried about the autonomous weapons of the future? Look at what's already gone wrong." Bulletin of the Atomic Scientists, 21 April 2021. https://thebulletin.org/2021/04/worried-about-the-autonomous-weapons-of-the-future-look-at-whats-already-gone-wrong/
51. Johnson, James. "Nuclear Brinkmanship in AI-Enabled Warfare: A Dangerous Algorithmic Game of Chicken." War on the Rocks, 28 September 2023. https://warontherocks.com/2023/09/nuclear-brinkmanship-in-ai-enabled-warfare-a-dangerous-algorithmic-game-of-chicken/
52. Sokolski, H. D., ed. Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice. Strategic Studies Institute, U.S. Army War College, 2004. https://apps.dtic.mil/sti/tr/pdf/ADA428336.pdf
53. Clapp, Sebastian. Defence and Artificial Intelligence. EPRS Briefing, PE 569.580, European Parliamentary Research Service, April 2025. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf
54. Nuclear Threat Initiative. "Transparency, Accountability and Assurance in Nuclear Security." March 20, 2012. https://www.nti.org/analysis/articles/transparency-accountability-and-assurance-nuclear-security/
55. Simmons-Edler, Riley; Dong, Jean; Lushenko, Paul; Rajan, Kanaka; Badman, Ryan P. "Military AI Needs Technically-Informed Regulation to Safeguard AI Research and its Applications." arXiv preprint arXiv:2505.18371v1, May 2025. https://arxiv.org/html/2505.18371v1
56. Khasru, Syed Munir; Gillwald, Alison; Sesan, 'Gbenga; Zondi, Siphamandla. International AI Governance: The Importance of G7-G20 Synergy. CIGI Policy Brief, April 2025. https://www.cigionline.org/static/documents/TF1_Khasru_et_al_rev.pdf

Endnotes

57. Organisation for Economic Co-operation and Development (OECD). OECD AI Principles. OECD, updated May 2024. https://www.oecd.org/en/topics/sub-issues/ai-principles.html
58. Cronberg, Tarja. “The militarisation of non-proliferation: Will the NPT survive?” European Leadership Network, 2025. https://europeanleadershipnetwork.org/the-militarisation-of-non-proliferation-will-the-npt-survive/
59. de Bourmont, Martin. “INF treaty: US withdraws from arms control agreement with Russia.” Al Jazeera, 2 August 2019. https://www.aljazeera.com/news/2019/8/2/inf-treaty-us-withdraws-from-arms-control-agreement-with-russia
60. Rautenbach, Peter. “On Integrating Artificial Intelligence With Nuclear Control.” Arms Control Association, Arms Control Today, September 2022. https://www.armscontrol.org/act/2022-09/features/integrating-artificial-intelligence-nuclear-control
61. Zhang, Jiayu. “China’s Military Employment of Artificial Intelligence and Its Security Implications.” The International Affairs Review (IAR-GWU), Summer 2020, Aug. 16, 2020. https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap
62. https://edition.cnn.com/2025/05/09/china/china-military-tech-pakistan-india-conflict-intl-hnk
63. State Council Information Office of the People’s Republic of China. “China’s National Defense in the New Era.” White paper, July 24, 2019.
https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html
64. C. Raja Mohan. “Why India cannot afford to repeat its nuclear weapons mistakes with AI.” The Indian Express, December 6, 2023. https://indianexpress.com/article/opinion/columns/c-raja-mohan-writes-why-india-cannot-afford-to-repeat-its-nuclear-weapons-mistakes-with-ai-9056025/
65. https://pmindiaun.gov.in/public_files/assets/pdf/statement_6sep.pdf
66. Greenstein, George. “A Gentleman of the Old School: Homi Bhabha and the Development of Science in India.” The American Scholar, vol. 61, no. 3, Summer 1992, pp. 409–419. https://www.jstor.org/stable/41212042
67. Carnegie Endowment for International Peace. “Striking Asymmetries: Nuclear Transitions in Southern Asia.” by Ashley J. Tellis, July 18, 2022. https://carnegieendowment.org/research/2022/07/striking-asymmetries-nuclear-transitions-in-southern-asia?lang=en
68. C. Raja Mohan. “Why India cannot afford to repeat its nuclear weapons mistakes with AI.” The Indian Express, December 6, 2023. https://indianexpress.com/article/opinion/columns/c-raja-mohan-writes-why-india-cannot-afford-to-repeat-its-nuclear-weapons-mistakes-with-ai-9056025/
69. Wittner, Lawrence S. Confronting the Bomb: A Short History of the World Nuclear Disarmament Movement. Stanford University Press, 2009. https://eacpe.org/app/wp-content/uploads/2014/02/Confronting-the-Bomb-BOOK-pdf.pdf
70. Perkovich, George. “Faulty Promises: The U.S.–India Nuclear Deal.” Carnegie Non-Proliferation / South Asia, PolicyArchive Report, September 2005.
71. NITI Aayog. National Strategy for Artificial Intelligence. Government of India, March 2023.
https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
72. Ministry of Defence, Government of India. “Enhancement of Capabilities of AI Technology.” Press Information Bureau, 01 August 2022. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1846937
73. Mohsin, Saleha. “Inside Project Maven, the US Military’s AI Project.” Bloomberg, February 29, 2024.https://www.bloomberg.com/news/newsletters/2024-02-29/inside-project-maven-the-us-military-s-ai-project
74. OECD / European Commission. STIP Compass – Interactive Dashboard entry 24943. OECD, 2023.
https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2023%2Fdata%2FpolicyInitiatives%2F24943
75. Bitzinger, Richard A.; Evron, Yoram; and Yang, Zi. “China’s Military–Civil Fusion Strategy: Development, Procurement, and Secrecy.” Asia Policy, Vol. 16, No. 1 (January 2021), pp. 1–64. The National Bureau of Asian Research, 2021. https://www.nbr.org/wp-content/uploads/pdfs/publications/ap16-1_china_mcf_rt_jan2021.pdf
76. C. Raja Mohan. “Why India cannot afford to repeat its nuclear weapons mistakes with AI.” The Indian Express, December 6, 2023. https://indianexpress.com/article/opinion/columns/c-raja-mohan-writes-why-india-cannot-afford-to-repeat-its-nuclear-weapons-mistakes-with-ai-9056025/
77. Hooda, Lt. Gen. Deependra Singh (Retd.). “Implementing Artificial Intelligence in the Indian Military.” Delhi Policy Group Policy Brief, 16 February 2023. https://www.delhipolicygroup.org/publication/policy-briefs/implementing-artificial-intelligence-in-the-indian-military.html

Endnotes

78. C. Raja Mohan. “Why India cannot afford to repeat its nuclear weapons mistakes with AI.” The Indian Express, December 6, 2023.
79. Arya.ai becomes first Indian startup to make it to international innovators list. The Times of India, 3 December 2015. https://timesofindia.indiatimes.com/business/india-business/arya-ai-becomes-first-indian-startup-to-make-it-to-international-innovators-list/articleshow/50025546.cms
80. Thaker, Naini. “SigTuple’s cutting edge AI tech hopes to democratise diagnostics.” Forbes India, June 27, 2023. https://www.forbesindia.com/article/startups/sigtuples-cutting-edge-ai-tech-hopes-to-democratise-diagnostics/86137/1
81. Times of India Business Desk. “AI shift: India’s IT majors embrace integration over invention, upskill workforce as global market booms.”The Times of India, June 29, 2025.
82. NITI Aayog. National Strategy for Artificial Intelligence. Government of India, March 2023. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
83. Department of Defence Production, Ministry of Defence. Artificial Intelligence in Defence. DDPMoD, November 2023. https://www.ddpmod.gov.in/sites/default/files/2023-11/ai.pdf
84. Csernatoni, Raluca. “Governing Military AI Amid a Geopolitical Minefield.” Carnegie Endowment for International Peace, 17 July 2024. https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en
85. UNIDIR Security and Technology Programme. Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security: An Evidence-Based Road Map for Future Policy Action. Geneva: UNIDIR, July 2025. https://www.unidir.org/wp-content/uploads/2025/07/UNIDIR_AI_military_domain_implications_international_peace_security.pdf
86. Sile, LtCol. Jack (Retd.). “Artificial Intelligence as a Force Multiplier for Marines.” Marine Corps Gazette, April 2025. https://www.mca-marines.org/wp-content/uploads/Sile-Apr25-WEB.pdf
87. Niazi, Lal Khan. “Militarization of Artificial Intelligence and Implications for Global Security – A Strategic Theory Perspective.” Social Sciences Spectrum, vol. 4, no. 1 (2025): 21-29. https://doi.org/10.71085/sss.04.01.198
88. Stockholm International Peace Research Institute (SIPRI). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk — Volume I: Euro-Atlantic Perspectives. Edited by Vincent Boulanin, May 2019. https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf
89. Lawrence Livermore National Laboratory, Center for Global Security Research. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. CGSR-AI_BattlefieldWEB, August 2024. https://cgsr.llnl.gov/sites/cgsr/files/2024-08/CGSR-AI_BattlefieldWEB.pdf
90. Boulanin, Vincent, et al. The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume I — Euro-Atlantic Perspectives.SIPRI Policy Paper, May 2019. https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf
91. Bichard, Connor J.; Dafoe, Allan; Macdonald, David; & Zavgorodnii, Yulian. “Strategic insights from simulation gaming of AI race dynamics.” Technological Forecasting and Social Change, 2025. https://www.sciencedirect.com/science/article/pii/S0016328725000254
92. Vaynman, Jane. “Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control.” Texas National Security Review, vol. 4, no. 4, Fall 2021, pp. 33–56, https://tnsr.org/2021/09/better-monitoring-and-better-spying-the-implications-of-emerging-technology-for-arms-control/
93. Viveros Álvarez, Jimena Sofía. “The Risks and Inefficacies of AI Systems in Military Targeting Support.” ICRC Humanitarian Law & Policy Blog, 4 Sept. 2024, https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/
94. Kwik, Jonathan, and Tom M. van Engers. “Algorithmic Fog of War: When Lack of Transparency Violates the Law of Armed Conflict.” Journal of Future Robot Life, vol. 2, no. 1–2, 2021, pp. 1–24, doi:10.3233/FRL-200019.
95. Hertog, Stefano, and Jonas Höss. “Autonomous Weapons and the Future of Warfare.” Futures & Foresight Science, vol. 2, no. 4, 2020, https://doi.org/10.1016/S2214-2126(20)30862-0

C-21, 3rd Floor, Qutub Institutional Area, New Delhi, India - 110016.
Phone: 011-43104566 | Email: office@csdronline.com | Web: www.csdronline.com | Twitter:@CSDR_India